POLYPUBLIE
Polytechnique Montréal

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Titre: Title:	Défense contre l'attaque d'analyse de trafic dans les réseaux de capteurs sans fil (WSN)
Auteur: Author:	Salah-Eddine Benbrahim
Date:	2011
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Benbrahim, S.-E. (2011). Défense contre l'attaque d'analyse de trafic dans les réseaux de capteurs sans fil (WSN) [Master's thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/655/

Document en libre accès dans PolyPublie
Open Access document in PolyPublie

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/655/
Directeurs de recherche: Advisors:	Martine Bellaïche
Programme: Program:	Génie informatique

Ce fichier a été téléchargé à partir de PolyPublie, le dépôt institutionnel de Polytechnique Montréal
This file has been downloaded from PolyPublie, the institutional repository of Polytechnique Montréal

https://publications.polymtl.ca

UNIVERSITÉ DE MONTRÉAL

DÉFENSE CONTRE L'ATTAQUE D'ANALYSE DE TRAFIC DANS LES RÉSEAUX DE CAPTEURS SANS FIL (WSN)

SALAH-EDDINE BENBRAHIM
DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
AOÛT 2011

© Salah-Eddine BENBRAHIM, 2011.

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

DÉFENSE CONTRE L'ATTAQUE D'ANALYSE DE TRAFIC DANS LES RÉSEAUX DE CAPTEURS SANS FIL (WSN)

présenté par : BENBRAHIM, Salah-Eddine
en vue de l'obtention du diplôme de : Maîtrise ès Sciences Appliquées
a été dûment accepté par le jury d'examen constitué de :

M. PIERRE, Samuel, Ph.D., président.
Mme. BELLAÏCHE, Martine, Ph.D., membre et directrice de recherche.
M. QUINTERO, Alejandro, Doct., membre.

À mes très chers parents,
ma femme et mes enfants...

REMERCIEMENTS

Je tiens à remercier ma directrice de recherche Mme. Martine BELLAICHE, pour avoir assuré la direction de mes travaux, pour la qualité de son encadrement, ses remarques pertinentes, son soutien, et qui de part son expérience, m'a permis de finaliser ce travail grâce à son suivi efficace et ses conseils avisés.

Je remercie aussi les membres du jury qui ont accepté d'étudier ce mémoire.

Une pensée particulière est adressée à ma mère, ma femme et mes enfants, pour leur soutien inconditionnel tout au long de la période d'études.

Merci à tous.

RÉSUMÉ

Le réseau de capteurs sans fil WSN possède deux modes de fonctionnement, le mode infrastructure où un point d'accès lie les capteurs entre eux, et le mode ad-hoc où les capteurs sont liées directement entre eux. L'architecture de communication entre les capteurs d'un réseau WSN est basée sur différentes couches comme la couche d'application, de transport, de réseau, de liaison/MAC, et la couche physique. Chaque couche a ses propres protocoles de transmissions de données qui peuvent être simulés avec divers outils comme "NS2", "SensorSimil", "SSFNet", "J-Sim", "SENSE", "TOSSIM" et "GlomoSim".

Les réseaux WSN sont omniprésents dans divers domaines tels que la santé et le secteur militaire. Ces réseaux ont plusieurs avantages comme la facilité de déploiement massif de leurs capteurs, la protection et la supervision des applications critiques, et le fonctionnement en continu du réseau à temps réel.

Cependant, les attaques de dénis de service, comme l'attaque d'analyse de trafic, peuvent avoir des impacts négatifs sur les applications critiques des réseaux WSN, minimisant ainsi la sécurité au sein de ces réseaux. Donc, il est important de sécuriser ces réseaux afin de maintenir leur efficacité. Comme les capteurs sont incapables de traiter leur sécurité d'une manière autonome, une approche globale de la sécurité contre les attaques devient indispensable.

Les attaques dans les réseaux WSN, dont les dénis de service font partie, ciblent les informations en circulation. Ces dénis de service se caractérisent par un type d'utilisateur, par un type de service partagé, et par un temps d'attente raisonnable. Plusieurs mécanismes de sécurité de réseaux WSN sont utilisés afin de contrer les effets des dénis de service.

Notre étude s'intéresse spécifiquement à l'attaque d'analyse de trafic. Elle en décrit la démarche aboutissant à la localisation de la station de base pour ensuite l'isoler du reste du réseau, et rendre ainsi le réseau WSN désuet. Notre technique de protection utilisée est la génération aléatoire de faux trafic autour d'une fausse station de base mobile. Ce faux trafic est généré par des capteurs collaborateurs, qui injectent dans le réseau WSN du faux trafic à destination de la fausse station de base. L'élection de la fausse station de base et des capteurs collaborateurs est aléatoire. La validation de la technique proposée se fait avec une simulation J-Sim. Notre technique est faisable dans un réseau doté d'une station de base unique, et son application peut s'étendre à un réseau muni de plusieurs stations de base. L'inconvénient

de notre solution est la consommation additionnelle élevée des ressources énergétiques des capteurs du réseau WSN protégé.

En conclusion, les réseaux WSN peuvent être protégés de l'attaque d'analyse de trafic par l'utilisation d'une partie de leurs réseaux pour générer du faux trafic perturbant ainsi le mouvement de l'attaquant.

Mots clés : Réseaux de capteurs sans fil (WSN), Dénis de service (DoS), Sécurité de WSN, Attaque d'analyse de trafic, Fausse station de base mobile.

ABSTRACT

The WSN has two modes, infrastructure mode where an access point connects the sensors between them, and the ad-hoc mode where the sensors are connected together directly. The communication architecture between sensors in a WSN is based on various layers: application, transport, network, link/MAC, and physical layer. Every layer has its own protocols of data transmissions, which can be simulated with different tools like: "NS2", "SensorSimil", "SSFNet", "J-Sim", "SENSE", "TOSSIM", and "GlomoSim".

These WSN are omnipresent in several domains like health and military sectors. These networks have several advantages like their easiest massive deployment of its sensors, the protection and the supervision of the critical applications, and the nonstop functioning of the real time network.

However, denials of service attacks, like traffic analysis attack can have negative impacts on the critical applications of the WSN, thus minimizing safety within these networks, so these networks require an important security against these DoS to maintain its efficiency. As sensors are incapable of handling their own security in an autonomous way, the security in the WSN becomes difficult, and a global approach of the security against attacks becomes indispensable.

Attacks in the WSN network, including denials of services, target information in circulation. These denials of services are characterized by user type, by shared service type, and by reasonable latency. Several mechanisms of securing WSN are used, in order to counter the effects of denials of services.

Our study discusses particularly the traffic analysis attack. It describes the approach leading to the localization of the base station, for then insulating it from the network, and thus making WSN network obsolete. Our protection technique uses the random generation of false traffic, around a mobile false base station. This false traffic is generated by collaborator sensors, which inject the false traffic to the false base station. The election of the false base station and the collaborator sensors is random. This technique is validated with J-Sim that confirms its good running. This base station protection technique is feasible in a network equipped with a single base station, and its application can be extended to a network provided

with several base stations. The disadvantage of our solution is the high additional energy resource consumption of the sensors of a protected WSN.

In conclusion, WSN can be protected from the analysis traffic attack by using a portion of the network sensors to generate a false traffic, thus disrupting the movement of the attacker.

Keywords : Wireless sensors Network (WSN), Denials of services (DoS), WSN security, Traffic analysis attack, Mobile false base station.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

AAT	Attaque d'analyse de trafic (Traffic analysis attack).
API	L'interface de programmation des applications (Application Programming Interface).
CAN	Convertisseur Analogique-Numérique.
Dénis de service	Refus de fournir une fonctionnalité.
DoS	Déni de service (Denial of Service).
DSR	Routage dynamique de source dynamique (Dynamic Source Routing).
EAR	Ecouter et enregistrer (Eavesdrop And Register).
GlomoSim	Simulation de système mobile d'informations (Global Mobile Information System Simulation).
IEEE	Instituts des ingénieurs électriques et électroniques (Institute of Electrical and Electronics Engineers).
J-Sim	Simulateur en Java (Java Simulator).
LEACH	Hiérarchie par grappes adaptative en basse énergie (Low-Energy Adaptive Clustering Hierarchy).
NS2	Simulateur de réseau 2 (Network Simulator 2).
OSI	Interconnexion de Systèmes ouverts (Open Systems Interconnection).
QoS	Qualité de Service (Quality of Service).
SAR	Affectateurs séquentielle de routage (Sequential Assignment Routing).
SENSE	Simulateur et l'émulateur de réseaux de capteurs (Sensor Network Simulator and Emulator).
SSFnet	Scalable Simulation Framework for network.
SMP	Protocol de gestion de capteurs (Sensor Management Protocol).
SMECN	Petite réseau de communication minimale d'énergie (Small Minimum Energy Communication Network).
SMACS	Auto-organisation du MAC des réseaux de capteurs (Self-organizing Medium Access Control for Sensor networks).
SQDDP	Protocole d'interrogation de capteur et de diffusion des données (Sensor Query and Data Dissemination Protocol(
TADAP	Protocole d'affectation des tâches et de la publicité des données (Task Assignment and Data Advertisement Protocol).
TCL	Outil de gestion des ordres (Tool Command Language).
TinyOS	Système d'exploitation minuscule (Tiny Operating System).

UDP-Like	Protocole ressemblant au Datagramme d'Utilisateur (User Datagram Protocol Like).
WSN	Réseau de capteurs sans fil (Wireless Sensor Network).

CHAPITRE 1

INTRODUCTION

Notre présente étude s'intéresse à l'attaque d'analyse de trafic (AAT), et met en place une nouvelle techniques de défense contre cette attaque par l'introduction d'une fausse station de base mobile recevant de faux trafics.

Ce chapitre s'articule en quatre parties qui sont successivement, (i) le contexte de l'attaque d'analyse de trafic AAT, (ii) la défense d'un réseau WSN contre ce type d'attaque AAT, (iii) l'esquisse de la méthodologie de notre nouvelle solution de défense proposée, et (iv) enfin le plan de ce mémoire.

1.1 Contexte

La demande actuelle pour les réseaux sans fil a permis leur intégration dans plusieurs domaines tels que la surveillance militaire, environnementale, et médicale.

Chaque capteur fonctionne comme une station de capture de données. Ces données sont ensuite envoyées et traitées par une station de base. Le déploiement des capteurs peut être prédéterminé ou bien aléatoire (par exemple en les jetant d'un avion). Ces types de déploiement exigent des stratégies différentes pour le routage des informations et leurs sécurités. Les capteurs peuvent avoir des rôles différents, ainsi que des capacités différentes et hétérogènes selon les applications des réseaux WSN. Ainsi, la fiabilité et la sécurité des informations véhiculées dans un réseau WSN dépendent de plusieurs paramètres, dont les ressources énergétiques de chaque capteur, les types des protocoles utilisées pour le routage, et le transport de ces données.

Les réseaux de capteurs WSN font face à plusieurs attaques qui menacent, entre autre, la station de base. La mise en panne de cette station de base peut mettre en péril tout le réseau WSN, d'où l'importance de protéger cette station de base contre des attaques comme celle d'analyse de trafic AAT. Cette attaque ananlyse le trafic dans un réseau WSN, et en déduit la position de la station de base pour éventuellement la détruire.

1.2 Éléments de la problématique

Les réseaux WSN sont vulnérables à plusieurs attaques. Certaines attaques se concentrent sur l'isolement de la station de base, et ont pour incidence l'arrêt total ou partiel des fonctionnalités du réseau, d'où la nécessité de la protection de la station de base pour le bon fonctionnement d'un réseau WSN.

L'attaque d'analyse de trafic AAT est l'une des attaques de dénis de service, où l'attaquant évalue les volumes d'informations véhiculées sur le réseau, en faisant abstraction de leurs contenus, et en repère la région de la station de base par son important volume de données, car tous les capteurs du réseau envoient leurs informations vers cette région.

La problématique de notre présente étude est d'empêcher un attaquant d'analyse de trafic de localiser la station de base par comptabilisation des informations dans le réseau WSN.

1.3 Objectifs de la recherche

Notre étude présente une nouvelle technique de sécurisation d'un réseau WSN contre l'attaque d'analyse de trafic AAT, en utilisant une fausse station de base mobile. Plusieurs objectifs sont pris en considération :

1. La sécurisation de la station de base.
2. La perturbation de la démarche de l'attaquant de l'analyse de trafic en générant du faux trafic.
3. L'optimisation de l'utilisation des ressources énergétiques.
4. La fiabilité des données reçues par la station de base.

Une simulation du modèle proposé avec l'outil J-Sim [6] permet de valider la solution mise en place, en renforçant la sécurité d'un réseau WSN contre l'attaque de déni de service appelée "**A**ttaque d'**A**nalyse de **T**rafic" (AAT), qui localise la station de base du réseau WSN, pour éventuellement l'isoler du reste du réseau.

1.4 Esquisse de la méthodologie

Nous proposons dans cette étude une nouvelle approche de sécurisation de la station de base contre l'attaque d'analyse de trafic AAT. Cette approche repose sur la perturbation de la démarche de l'attaquant de l'analyse de trafic via la génération de faux trafic, tout en respectant les contraintes des capteurs en ressources énergétiques et en puissance de calcul. La vérification de la solution proposée est élaborée par simulation J-Sim [6]..

Nous générons du faux trafic en provenance d'une partie des capteurs du réseau WSN. Ce faux trafic est acheminé vers une fausse station de base mobile élue parmi les capteurs du réseau. Ainsi, le volume du trafic est accentué autours de cette fausse station de base. L'attaquant de l'analyse de trafic AAT se déplace vers la fausse station de base en s'éloignant de la vraie station de base. Grâce à cette technique, nous perturbons la démarche de l'attaquant en déplaçant la fausse station de base, créant ainsi des régions de trafic élevé mobiles.

1.5 Plan du mémoire

Ce mémoire est composé de huit chapitres. Le chapitre 1, est l'introduction qui présente les divers aspects de cette étude : contexte, objectif, méthodologie, et plan du mémoire. Le chapitre 2, décrit les réseaux de capteurs WSN. Le chapitre 3, présente les attaques dans les réseaux WSN. Le chapitre 4, met l'accent sur l'attaque d'analyse de trafic. Au chapitre 5, nous présentons la configuration de notre réseau WSN simulé. Au chapitre 6, nous introduisons notre nouvelle technique de défense contre l'attaque d'analyse de trafic AAT. Au chapitre 7, nous validons notre nouvelle technique. Enfin au chapitre 8, nous concluons notre étude et nous présentons les nouvelles perspectives d'amélioration des résultats de la technique proposée de défense contre l'attaque d'analyse de trafic.

CHAPITRE 2

RESEAUX DE CAPTEURS SANS FIL WSN

L'objectif d'un réseau de capteurs sans fil (WSN) [7] est la récolte de données et d'informations afin de les transmettre via des capteurs en utilisant des supports sans fil. Ces informations peuvent être des données environnementales, médicales ou militaires dans des conditions géographiques difficiles.

2.1 Description des réseaux de capteurs sans fil (WSN)

Le réseau de capteurs sans fil WSN est composé de plusieurs capteurs déployés dans des régions où l'on cherche à récolter des données. Les algorithmes et les protocoles [8] dans ces réseaux de capteurs doivent s'auto-organiser. Les capteurs doivent coopérer entre eux et peuvent traiter une partie de l'information localement (via leurs microprocesseurs) avant de transmettre le résultat. Le réseau WSN est différent des réseaux traditionnels par :

- Le nombre élevé de ses capteurs,
- Leur concentration,
- Leur prédisposition aux pannes,
- Leur intercommunication par diffusion au lieu de la communication point-à-point.

Un capteur est composé de plusieurs unités (voir figure 2.1) :

- Une unité de captage de données pour accueillir les données et les convertir,
- Une unité de stockage et de traitement de données,
- Une unité de communication pour émettre et recevoir les données,
- Un système de localisation pour identifier l'emplacement d'un capteur,
- Un mobilisateur pour déplacer le capteur,
- Une unité d'énergie pour gérer l'énergie d'un capteur.

Ces unités permettent alors aux capteurs de communiquer entre eux selon plusieurs approches :

- Par approche évènementielle,
- Par contrôle continu,
- Par centralisation de données,
- Par distribution de données.

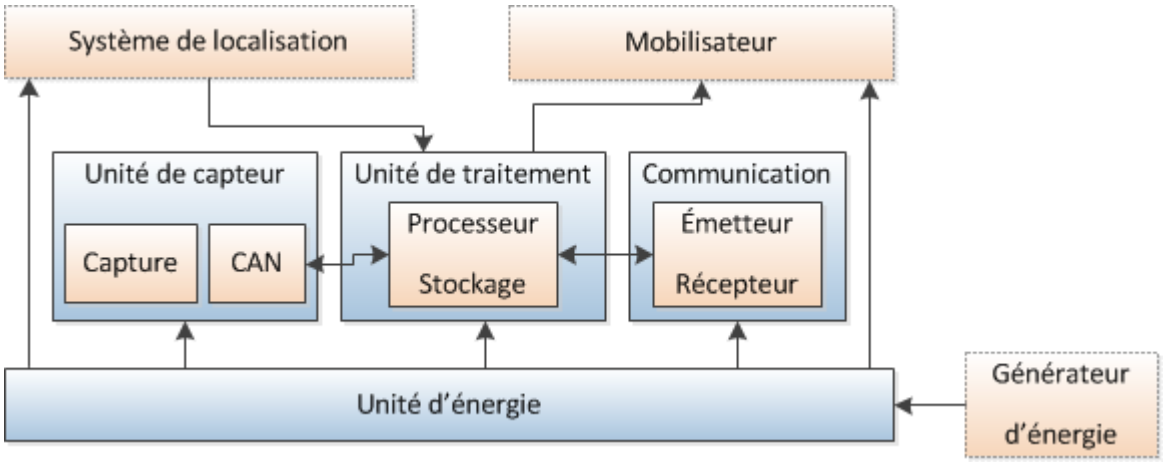

Figure 2.1 Structure d'un capteur [2].

2.2 La communication entre les capteurs

Les stratégies de communication entre les capteurs dépendent de plusieurs paramètres tels que les applications et les objectifs du réseau à mettre en place. Cette communication peut être appréhendée de plusieurs façons :

- La démarche événementielle permet d'envoyer des données suite à une requête ou une capture de données. Le capteur est souvent en mode repos ce qui lui permet d'économiser son énergie.
- La démarche de contrôle continue permet d'envoyer des données régulièrement. Elle permet de mieux gérer la consommation de l'énergie.
- La centralisation des données permet d'intercepter les événements, et les envoyer aux "cluster-Head" [9] qui captent toutes les informations des autres capteurs du "cluster" [9]. Les capteurs y sont souvent organisés dans des ensembles "clusters" (ensemble de capteurs similaires) (voir figure 2.2).
- La distribution des données permet de localiser les capteurs voisins, d'effectuer des calculs, et de prendre des décisions collectivement. Les capteurs y sont souvent organisés en mailles.

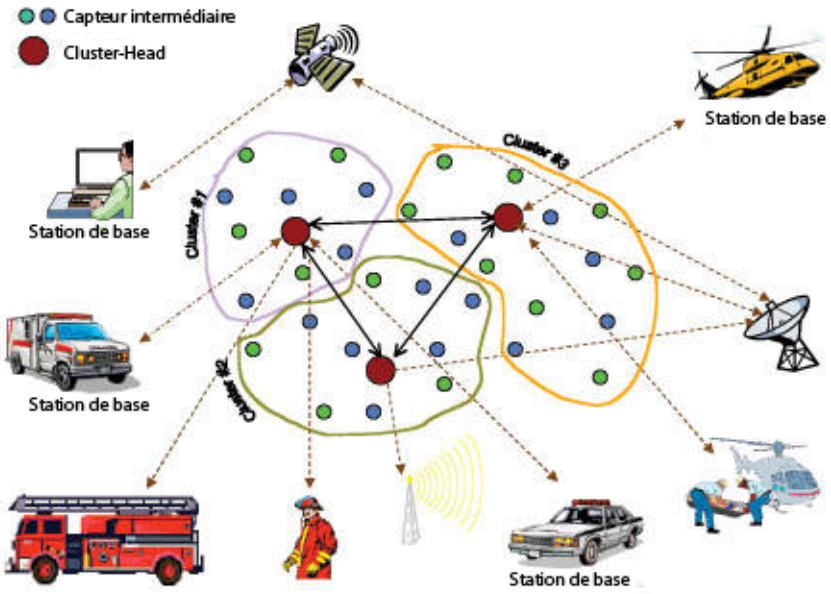

Figure 2.2 Exemple d'organisation des capteurs en "clusters" [2].

2.3 Causes de la vulnérabilité des réseaux WSN

Les réseaux de capteurs sans fil (WSN) sont vulnérables de part les éléments suivants :

- Une énergie limitée.
- Une mémoire limitée.
- Une puissance de calcul limitée.
- Une communication très variable entre une grande quantité de capteurs.
- Une panne facile à produire.
- Une concentration élevée.
- Un moyen de transmission à faible fiabilité et à interception facile par autrui.
- Une fragilité physique.

Ainsi, la sécurité des réseaux de capteurs sans fil reste à améliorer.

2.4 Les caractéristiques des réseaux de capteurs sans fil (WSN)

Les réseaux de capteurs sans fil (WSN) [7] possèdent plusieurs propriétés dont :

- La durée de vie limitée des capteurs car ils ont des ressources limitées en calcul, en mémoire, et en énergie.
- La densité élevée de capteurs WSN qui fonctionnent en communication multi-sauts.

- L'absence d'un identifiant global pour les capteurs qui sont reconnus par leurs localisations.
- Le fonctionnement des capteurs intermédiaires comme des agrégats et des calculateurs.
- La coopération entre les capteurs pour résoudre une tâche de haut niveau.
- Le fonctionnement en mode "plusieurs-à-un", où les capteurs envoient des informations à la station de base, et le fonctionnement en mode "un-à-plusieurs", au niveau duquel la station de base envoie des données aux différents capteurs.

2.5 La fiabilité et la congestion des données dans les WSN

Il existe trois types de messages dans le réseau de capteurs sans fil (WSN) :

- Les données des capteurs vers la station de base.
- Les données de contrôle ou de gestion de la station de base vers les capteurs.
- Les codes des tâches ou de reprogrammation de la station de base vers les capteurs.

Dépendamment du sens du flux de données des applications, le transport des données peut être classé en trafic de "capteurs-vers-la station de base" ou trafic de "station de base-vers-les capteurs".

La fiabilité des données [10] de réseau de capteur sans fil WSN dépend du sens des communications, et du type de l'application utilisée. Cette fiabilité peut être garantie ou stochastique. Certaines applications ont besoin d'une fiabilité garantie où chaque paquet doit être reçus correctement (fiabilité des paquets), alors que d'autres applications n'ont besoin que d'une fiabilité stochastique, par exemple, un événement peut être considéré comme fiable si un certain pourcentage de ses paquets est correctement reçu par la station de base (fiabilité de l'application).

La congestion [11] dans les réseaux de capteurs sans fil WSN apparait principalement quand des capteurs envoient des données à la station de base dans une topologie "plusieurs-vers-un".

2.6 Les caractéristiques des protocoles de communications dans les réseaux de capteurs sans fil WSN

Les protocoles de communications entre les capteurs des réseaux WSN prennent en considération plusieurs éléments dont :

- La minimisation de la consommation en énergie : les capteurs sont de petites tailles, et équipés de petites batteries d'énergie. Dans un réseau multi-sauts, les capteurs jouent à la fois le rôle de routeur et de source de données, pour ces raisons les chercheurs

s'intéressent de plus en plus à l'optimisation de la consommation de l'énergie, de la conception des algorithmes, et des protocoles de communication dans WSN.

- La variabilité de la topologie : les capteurs de réseaux WSN sont nombreux (leurs densités, allant jusqu'à 20 capteurs/m3), ce qui complique leur maintenance. Les capteurs peuvent être déployés un par un ou en bloc dans une région. Après leurs premiers déploiements, ils peuvent modifier leurs localisations.
- La tolérance aux pannes d'un capteur : un capteur peut facilement tomber en panne par manque d'énergie ou à cause d'une destruction physique, le réseau de capteurs sans fil WSN doit continuer à fonctionner normalement malgré cette défaillance.
- La communication à distance sécurisée : La communication directe avec les capteurs peut s'avérer difficile, il est donc judicieux de les commander à distance. Cependant, ce mode de transmission à distance entraine une augmentation du temps de communication.
- La diminution des coûts de déploiement des capteurs : étant donné le nombre élevé de capteurs dans un réseau sans fil WSN, le coût individuel de chaque capteur doit être le plus bas possible afin de justifier son utilisation par rapport à un réseau sans fil traditionnel.
- La spécification applicative : une application peut avoir besoin de plus de ressources pour répondre à ses propres objectifs.
- L'environnement de déploiement : les capteurs peuvent être déployés dans un camp ennemi, dans un océan, dans un immeuble dense, etc.
- Le support de communication : les capteurs peuvent communiquer en utilisant plusieurs types de signaux radio (Bluetooth pour AMPS), l'infrarouge ou les médias optiques.

2.7 Les protocoles de communications des réseaux de capteurs sans fil WSN

Actuellement, il existe deux protocoles de transport majeurs sur internet : UDP et TCP. Le protocole UDP ne fournit ni la fiabilité ni le contrôle de congestion, il n'est donc pas considéré comme un protocole approprié pour le transport d'information dans les réseaux WSN. Alors que le protocole TCP fournit une communication fiable "reliable end-to-end protocol", celui-ci est plus répandu dans le transport sur internet.

Le TCP ne peut pas être utilisé pour les réseaux sans fil multi-sauts à cause de la surconsommation d'énergie. Le TCP requiert une adresse unique pour un capteur, par opposition aux réseaux WSN où les capteurs ne peuvent pas avoir une adresse unique, mais seulement une adresse basée sur leurs attributs "attribute-based addressing".

Plusieurs protocoles [8] de communications existent pour les réseaux sans fil classiques. Cependant, les réseaux de capteurs sans fil WSN sont incompatibles avec ces protocoles à cause de leurs topologies variables et de leur faiblesse en énergie. Les protocoles compatibles avec les réseaux de capteurs sans fil (WSN) sont organisés en couches.

2.7.1 Les protocoles de la couche application

Il existe plusieurs protocoles [12] pour la couche application dont :

- Sensors management protocol (SMP) est un protocole utilisé par l'administrateur pour communiquer avec les capteurs en utilisant leurs attributs de nomenclature et leurs localisations.
- Task Assignment and Data Advertisement Protocol (TADAP) assigne des tâches aux capteurs pour une meilleure coordination du routage, et de la collecte d'informations.
- Sensors Query and Data Dissemination Protocol (SQDDP) permet à l'utilisateur de gérer les requêtes envoyées ou reçues des capteurs.

2.7.2 Les protocoles de la couche transport

Il existe plusieurs protocoles pour la couche transport dont :

- User Datagram Protocol Like (UDP-Like) [10] ressemble au protocole UDP, mais prend en considération la limite en énergie des capteurs.
- Event-to-sink transport protocol [13] s'exécute au niveau de la station de base, et permet d'identifier les capteurs du réseau en minimisant l'utilisation de l'énergie.
- Sink-to-sensors transport protocol permet de réduire le trafic dans le réseau, et de minimiser ainsi la dépense en énergie des capteurs.
- Small Minimum Energy Communication Network (SMECN) [14] permet de trouver un sous-réseau de communication efficace optimal en énergie.
- Low-Energy Adaptive Clustering Hierarchy (LEACH) [15] permet aux "Clusters-Head" de collecter des données, de les agréger, puis de les envoyer à la station de base.
- Sequential Assignment Routing (SAR) [16] permet de trouver un cheminement possible pour envoyer des données selon leurs priorités, selon la consommation de l'énergie, et selon la qualité de service (QoS).

2.7.3 Les protocoles de la couche liaison

Il existe plusieurs protocoles pour la couche liaison dont :

- Self-organizing Medium Access Control for Sensors networks (SMACS) [17] permet aux capteurs de se construire un réseau de communication sans faire appel à un capteur

spécial "Cluster-Head". Avec ce protocole, les capteurs communiquent entre eux avec des fréquences sans limites de bande passante. Ces capteurs se mettent au repos lorsqu'ils n'ont pas de données à envoyer.
- Eavesdrop And Register (EAR) [18] permet d'établir et de libérer une connexion.

2.8 Les outils de simulation des réseaux de capteurs WSN

Des simulateurs payants ou gratuits, dont certains sont listées ci-dessous, sont disponibles pour tester le comportement des réseaux de capteurs WSN en modélisant chaque capteur, chaque station de base, et chaque protocole de communication, ensuite un trafic est généré dans le réseau simulé soit à partir des capteurs vers la station de base ou inversement :

- NS2 est l'outil le plus répandu et le plus utilisé. Il profite d'un grand support technique auprès de ses utilisateurs, cependant, ce simulateur souffre des erreurs de dépassement de mémoire lors de la conception des grands réseaux de capteurs sans fil WSN.
- SensorSim [19] est une extension du simulateur NS2 pour les réseaux de capteurs sans fil WSN. Il gère de façon dynamique le fonctionnement des capteurs, cependant, comme NS2, il souffre de dépassement de mémoire lors de l'utilisation des grands réseaux de capteurs sans fil WSN.
- SSFNet est capable de gérer des réseaux de capteurs sans fil WSN de grande taille avec un bon temps de traitement, cependant, les modèles des protocoles utilisés ne sont pas détaillés.
- J-Sim est un outil gratuit utilisant des scripts comme TCL, Phyton et Perl. Il peut traiter des réseaux de grandes tailles et comporte des librairies spécifiques pour les réseaux de capteurs sans fil WSN, cependant, il définit une topologie fixe, ce qui limite son utilisation pour la conception de nouveaux protocoles.
- SENSE peut traiter des réseaux de grande taille, et gère bien la dépendance des modules et la réutilisabilité des composants, cependant, il n'est pas bien documenté et gère mal les interactions entre les composants internes.
- TOSSIM permet de simuler d'une manière évolutive les réseaux de capteurs sans fil WSN, cependant il ne fonctionne qu'avec le système d'exploitation "TinyOS" installé dans un capteur.

2.9 Les contraintes de sécurité dans les réseaux de capteurs sans fil WSN

Il existe deux catégories de contraintes de sécurité dans les réseaux de capteurs sans fil WSN. La première contrainte dépend des limites des ressources d'un capteur, alors que la seconde est liée aux types de support de communication du réseau de capteurs WSN.

- Les contraintes liées aux ressources : la mise en sécurité dans les réseaux de capteurs WSN demande une bonne quantité en ressources énergétiques, en mémoire et en stockage. Ainsi, avant la mise en place d'un système de cryptographie, il est indispensable d'étudier son influence sur les ressources du réseau WSN.
- Les contraintes liées aux types de supports : les réseaux de capteurs WSN utilisent des ondes pour transmettre les données. Il est difficile de protéger ce support de communication aussi efficacement que le support filaire.

2.10 Conclusion

Au cours de ce chapitre, nous décrivons les réseaux de capteurs WSN, les communications entre ses capteurs, leurs vulnérabilités, leurs protocoles de communications, leurs contraintes de sécurité, et les outils de simulation.

Les réseaux de capteurs WSN sont exploités dans plusieurs domaines, cependant ils présentent des vulnérabilités vis-à-vis de plusieurs types d'attaques, à cause de leurs limites en énergie, en mémoire, et en puissance de calculs.

Dans le chapitre suivant, nous introduisons les attaques de dénis de service et les défenses dans les réseaux de capteurs WSN.

CHAPITRE 3

REVUE DE LITTTERATURE DES ATTAQUES DE DÉNIS DE SERVICES ET DES DÉFENSES DANS LES RESEAUX DE CAPTEURS SANS FIL (WSN)

Ce chapitre permet de définir les différents types d'attaques et de défense (y compris les dénis de service) qui menacent les constituants des réseaux de capteurs sans fil WSN et leurs fonctionnalités.

Une **attaque** peut être définie comme une tentative d'accès non autorisé à un service, une ressource ou une information, ou bien la tentative de compromettre l'intégrité, la disponibilité, ou la confidentialité du réseau.

Un **déni de service** est le résultat de toute action susceptible d'empêcher une partie d'un réseau de capteurs WSN de fonctionner correctement ou en un temps opportun. La définition de déni de service (DoS) comprend trois composantes : les utilisateurs autorisés, un service partagé, et un temps d'attente maximum [20]. Les utilisateurs autorisés sont réputés refuser un service à d'autres utilisateurs autorisés, quand ils les empêchent d'utiliser un service partagé après un temps d'attente maximum.

3.1 La taxonomie des attaques dans les réseaux de capteurs WSN

La taxonomie (voir figure 3.1) permet de classifier les dénis de service. Elle permet de gérer le risque d'attaque en identifiant les vulnérabilités exploitées par l'attaquant d'un service ou d'une couche.

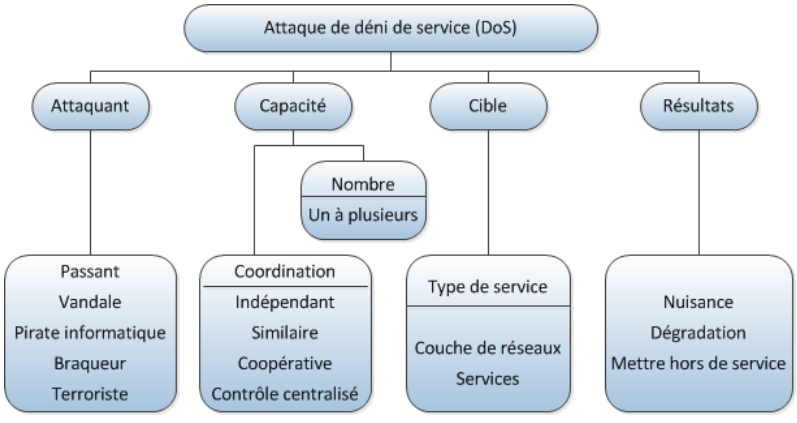

Figure 3.1 La taxonomie de déni de service dans les réseaux de capteurs sans fil (WSN) [3].

3.2 Description des attaquants

En général, plus l'attaquant dispose de ressources, plus la défense est coûteuse. La connaissance de la capacité de l'attaquant permet de définir au mieux la défense. La conception de réseaux de capteurs WSN doit prendre en considération les menaces les plus fréquentes en énumérant les capacités des attaquants (leur nombre, leur coordination, leur capacité technique et leur intérêt d'influence).

Plusieurs attaquants peuvent menacer un réseau au même moment d'une manière autonome ou en coordination, afin de réaliser une attaque commune rendant la défense difficile. La définition des capacités techniques des attaquants est importante pour connaitre la nature de leur menace, par exemple un attaquant peut seulement recevoir la transmission de données, mais il peut aussi se présenter comme un capteur légal du réseau, et avoir accès à la totalité des services du réseau.

L'attaquant peut avoir accès à tout le réseau en utilisant la diffusion, il peut aussi n'avoir accès qu'à une certaine région du réseau pour influencer son comportement. La cible et son importance sont des éléments clés d'une attaque d'un service ou d'une couche. L'attaque d'une couche basse est plus importante, car elle affecte les autres couches au dessus. Plusieurs services peuvent être attaqués, tels que la localisation, la synchronisation temporelle, et la gestion d'énergie. Les services critiques doivent être défendus plus que les services optionnels, car le mauvais fonctionnement des composants critiques nuit au fonctionnement de l'ensemble du réseau.

Chaque attaquant appartient à une catégorie :

- Passant : avec une motivation spontanée, des ressources et des connaissances limitées,
- Vandale : avec une motivation de dommage des ressources et des connaissances limitées,
- Pirate informatique : avec une grande motivation d'accès, de curiosité et d'intérêt,
- Braqueur : avec une grande détermination et des ressources limitées,
- Terroriste : avec des ressources importantes et une grande détermination.

3.3 Les type des vulnérabilités des réseaux de capteurs sans fil WSN

Les vulnérabilités sont les faiblesses d'un réseau que l'attaquant exploite afin de gagner des privilèges. Il y a deux types de vulnérabilités dans un réseau de capteurs WSN :

- La vulnérabilité physique est un moyen d'attaque, qui permet à l'attaquant de changer en partie un capteur, en modifiant par exemple son code de programmation, ou en copiant les clés de protection afin de les réutiliser dans une nouvelle attaque. Un réseau de capteurs est vulnérable aussi aux modifications de son environnement, où un attaquant peut modifier les valeurs d'un capteur local, lui permettant ainsi d'avoir un accès aux

commandes de contrôle du réseau WSN.
– La vulnérabilité logique réside dans les programmes et les protocoles. Elle se présente sous quatre formes : (i) les défauts de conception, (ii) les défauts d'implémentation, (iii) les erreurs de configuration, et (iv) l'épuisement des ressources.

Les défauts de conception permettent l'utilisation d'un protocole qui viole le mode d'utilisation, tout en se conformant à la spécification du protocole. Par exemple, un manque d'authentification dans un protocole de gestion de puissance peut permettre de mettre n'importe quel capteur en sommeil à plusieurs reprises.

Les défauts d'implémentation sont des erreurs dans la construction de matériel ou dans le codage du logiciel. Par exemple, une erreur de dépassement de mémoire, peut entraîner une violation d'accès et une mise en panne.

Les défauts de configuration sont le résultat de défauts de paramétrages pour un attaquant.

L'épuisement des ressources est possible même si la conception, l'implémentation, et la configuration sont correctes. Un attaquant générant de grandes quantités de trafic peut inonder un des liens réseau de la victime. Une mauvaise authentification de l'allocation de mémoire ou de l'exécution de code peut également permettre à un attaquant de consommer les ressources du capteur subissant l'attaque, et de causer un DoS

Dans les sections suivantes, nous présentons plusieurs types d'attaques contre le réseau WSN pouvant réduire ses fonctionnalités utiles.

3.4 Les attaques des informations véhiculées dans le réseau WSN

Dans les réseaux de capteurs WSN, les capteurs reportent à la station de base les modifications de certaines valeurs et paramètres spécifiques. Cependant, ces informations en transition peuvent être altérées, bloquées ou aspirées. Comme l'attaquant a de grandes capacités physiques, il peut corrompre plusieurs capteurs à la fois, afin de modifier leurs contenus envoyés sur les liens du réseau.

3.5 Les types de déni de service

Les dénis de service (DoS) sont définis comme un mauvais fonctionnement des capteurs d'une manière intentionnée ou par action malveillante. Le déni de service peut ne pas résulter d'une attaque, mais d'un simple événement empêchant le fonctionnement normal d'un de ses services. Le déni de service le plus simple est d'empêcher le fonctionnement normal du capteur

victime en lui envoyant énormément de messages sans importance, et en interdisant l'accès aux autres utilisateurs. Les attaques de déni de service ciblent la réduction des capacités d'un réseau de capteurs sans fil. Les contraintes physiques de ces réseaux de capteurs, et la nature de leur environnement de déploiement, les rendent vulnérables aux attaques de dénis de service plus que tout autre type de réseau.

Il existe deux types d'attaques qui peuvent apparaitre à tous les niveaux des couches de réseau de capteurs WSN :

- L'attaque passive dûe aux capteurs égoïstes du réseau qui ne coopèrent pas avec les autres capteurs,
- L'attaque active où les capteurs malveillants endommagent le réseau.

Chaque couche du réseau de capteurs WSN a ses propres dénis de service.

- Au niveau de la couche physique, le déni de service (DoS) se présente comme une attaque "flooding" ou "Tampering".
- Au niveau de la couche liaison, le déni de service (DoS) peut se présenter comme une collision, un "Jamming" ou une attaque "Unfairness".
- Au niveau de la couche réseau, le déni de service (DoS) peut se présenter comme une attaque "Neglect and Greed", "Homing", "Misdirection", ou "Black hole".
- Au niveau de la couche de transport, le déni de service (DoS) est une attaque "Flooding" malveillante ou une "Desynchronisation".

Des solutions pour contrer les DoS existent, comme l'augmentation des ressources, l'authentification et l'identification du trafic.

3.5.1 Les dénis de service par couche dans les réseaux de capteurs WSN

Dans notre étude, les sept couches du modèle ouvert international (OSI) traditionnel sont réduites aux cinq couches suivantes : physique, liaison, réseau, transport et application (voir tableau 3.1). Certaines attaques se concentrent sur les aspects physiques des réseaux de capteurs, comme la couverture d'un capteur par une barrière acoustique qui réduit sa sensibilité. D'autres attaques peuvent concerner la faiblesse des protocoles de transports et de ses applications.

Les attaques surviennent en utilisant plusieurs techniques. Les pirates informatiques repèrent les vulnérabilités du réseau, et de ses constituants. Ces vulnérabilités peuvent être des

failles de conception, des failles du support de communication, ou des failles de l'environnement de déploiement.

Tableau 3.1 Les dénis de service par couche et leur défense [1]

La couche	L'attaque	Les défenses
Physique	Jamming	Détection et mise en sommeil
		Route autour des régions de Jamming
	Falsification des capteurs	Camouflage des capteurs
Liaison/MAC	Interrogation	Authentification
	Déni de sommeil	Détection et mise en sommeil
Réseau	Modification du contenu des messages de contrôle	Authentification
		Formation des grappes (clusters) sûrs
	Hello flooding	Le routage géographique
	Homing	Encryptage des entêtes
Transport	Synchronisation flooding	Les cookies de synchronisation
	Attaque de désynchronisation	Authentification de paquets
Application	Ecrasement de capteurs	L'agrégation de données
	DoS basé sur le chemin	Authentification des paquets
	Attaque de déluge	Authentification

3.5.2 Les dénis de service contre le "Clustering"

Le déploiement, des réseaux de capteurs WSN de grande taille, utilise parfois le "clustering" pour le routage du trafic en optimisant l'énergie, par agrégation des données au niveau du "Cluster-Head". L'attaquant peut profiter du "clustering" pour introduire un faux "cluster-Head" disposant d'une forte transmission et qui invite plusieurs capteurs à rejoindre une grappe inexistante (voir figure 3.2).

Kun Sun et al [21] proposent un protocole de distribution basé sur des grappes (clusters) qui permettent aux capteurs de communiquer avec leurs voisins en utilisant le cryptage par clés publiques. Ce mécanisme est basé sur la cryptographie asymétrique. Certains protocoles effectuent l'élection de "Cluster-Head" en se basant sur l'état des ressources telle que l'énergie résiduelle des capteurs.

L'attaque "homing" fait partie des attaques contre les réseaux de capteurs sans fil WSN munis de la technique de regroupement (clustering). Elle touche les capteurs importants d'un réseau, spécialement les "Cluster-Head" et les gestionnaires des clés cryptographiques. Ainsi

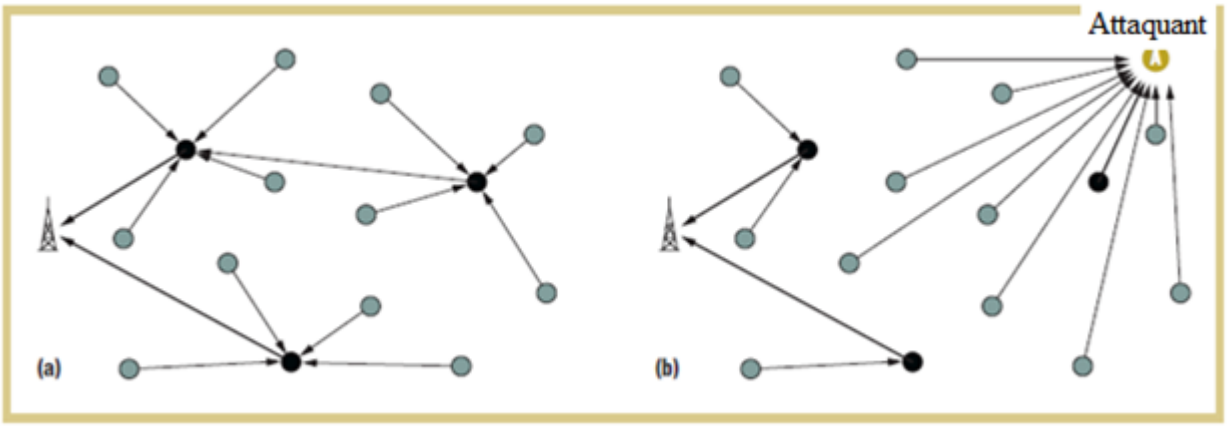

Figure 3.2 Influence d'un attaquant sur un réseau WSN : (a) un réseau avec cluster proprement dit (b) un réseau qui souffre d'un "Cluster-Head" malveillant [1].

le capteur malveillant peut attaquer les capteurs ou les inonder par des informations non nécessaires.

3.5.3 Les dénis de service au niveau des protocoles de routage dans les réseaux WSN

Il existe plusieurs protocoles de routage dans les réseaux ad-hoc, tels que le protocole du vecteur à distance à la demande (AODV), et le protocole de routage à source dynamique (DSR) ayant de bonnes performances. Cependant, il n'existe pas d'excellents protocoles de routage pour les réseaux WSN.

Les protocoles de routage sécurisés doivent répondre aux exigences suivantes : l'isolation des capteurs non-autorisés, la non-révélation de la topologie aux adversaires, la sécurisation des routes des messages, et l'identification des émetteurs des messages.

Pour sécuriser les protocoles de routage, il est indispensable de construire les éléments suivants :

- un mécanisme d'authentification avec des calculs légers et entêtes de petites tailles,
- la découverte de route sécurisée entre la source et la destination,
- la maintenance de routes qui permet de retourner les erreurs aux sources,
- la défense contre l'attaque «misdirection" (voir 3.6.5) et «flooding" (voir 3.6.9),
- l'isolation des liens malveillants.

3.6 Les dénis de service et les défenses

Nous décrivons dans cette section certains dénis de service et les moyens de sécurisation contre eux.

3.6.1 Neglect and Greed

C'est une forme simple de déni de service qui attaque la vulnérabilité du rôle routeur du capteur, en négligeant le routage de certains messages. Le capteur malveillant peut ainsi participer à des protocoles de bas niveaux, et peut même accuser réception des données du capteur expéditeur, mais par contre il perd ces données, ce capteur est appelé capteur négligeant ou capteur avide lorsqu' il donne une haute priorité pour ses propres messages.

Pour se défendre contre une attaque "Neglect and Greed", une technique basée sur le principe de "clustering" est utilisée, et se base sur le fait que les capteurs élisent un "Cluster-Head" en fonction des ressources énergétiques, et du coût de ses communications, ce capteur "Cluster-Head" détecte tout trafic inhabituel, et transmet l'information aux autres capteurs du groupe.

3.6.2 Homing

Dans la plupart des réseaux de capteurs WSN, certains capteurs ont des responsabilités spéciales, par exemple être leaders des communications de groupe, d'autres sont des gestionnaires de clés de cryptage. Ces capteurs attirent la curiosité, car ils fournissent des services critiques au réseau de capteurs WSN. Les protocoles de localisation exposent le réseau aux attaques de "homing", car un adversaire passif observe le trafic afin de connaître la présence et la localisation des ressources critiques, une fois ces capteurs spéciaux localisés, ils sont attaqués par des capteurs collaborateurs ou des adversaires mobiles.

Une approche de dissimulation permet de fournir la confidentialité dans les entêtes des messages et de leurs contenus [22].

3.6.3 Selective Forwarding

Dans les réseaux de capteurs WSN, chaque capteur participe au routage des données de ses capteurs voisins, et l'attaque "Selective Forwarding" exploite cette dépendance, afin de provoquer un déni de service (DoS), par exemple en négligeant de renvoyer un message, de la station de base ou à partir d'un autre capteur.

Pour se défendre de l'attaque "Selective Forwarding" , il est possible d'utiliser l'approche ***"diversity coding"*** [23] qui peut atténuer les effets de l'attaque en envoyant les messages codifiés sur plusieurs chemins.

3.6.4 Black holes

Le protocole basé sur le vecteur des distances (AODV) peut être attaqué par des dénis de service (DoS). Les capteurs indiquent des routes à coûts nuls aux autres capteurs ce qui constitue des "Black holes" de routage dans le réseau. Ainsi, au fur et à mesure que la publication des messages se propage, le réseau achemine plus de trafic dans leurs directions.

Une des approches de défense contre "Black holes" est de n'autoriser que les capteurs authentifiés à envoyer des informations des routes des messages [22].

La figure 3.3 montre un capteur malveillant qui s'est introduit entre des capteurs et une station de base afin de capter les paquets en transit entre eux.

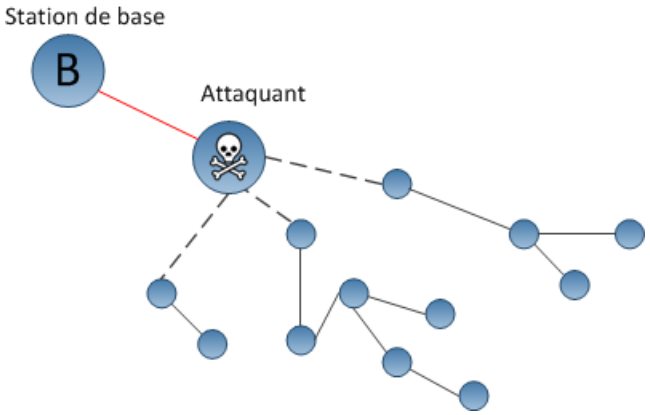

Figure 3.3 Une vue de l'attaque "Black holes" [4].

3.6.5 Misdirection

Misdirection est une attaque active, qui renvoie un message dans des mauvaises directions, en fabriquant une publication pour une route malveillante. Le protocole DSR est sensible à cette attaque. Un attaquant peut se forger une adresse source lors de l'envoi de requêtes, ainsi la réponse est retournée à un capteur victime. Cette méthode est utilisée afin d'affoler la victime ou bien de l'inonder.

Une des techniques de défense contre l'attaque de "Misdirection", est l'authentification des capteurs, ainsi les tables de routage sont mise à jour, en tenant compte des informations authentifiées des capteurs de la route [22].

3.6.6 Sink holes

Avec cette attaque, un capteur malveillant agit comme un "Black holes" afin de capter tout le trafic du réseau de capteurs WSN. L'attaquant écoute les requêtes des routes demandées par les capteurs victimes, puis il envoie un message à ces capteurs leur signifiant qu'il a à sa disposition le meilleur chemin vers la station de base. Une fois que le capteur malveillant s'est introduit dans le chemin entre le capteur victime et la station de base, il peut affecter l'acheminement du message comme il le souhaite (voir figure 3.3). Wood et al [22] décrivent l'attaque de "Sink holes" comme une attaque de fausses courtes routes.

Une des approches de défense contre cette attaque, est l'utilisation des algorithmes de routage résistants aux configurations arbitraires tel que le renvoi géographique (geographic Forwarding) [24]

3.6.7 Wormholes

L'attaque Wormholes [25] (voir figure 3.4) est une attaque critique, où l'attaquant énumère les paquets d'une localisation, et les transporte à une autre place. Cette attaque n'a pas besoin de compromettre un capteur du réseau de capteurs WSN, et peut même s'exécuter à la phase de découverte des capteurs voisins. Les attaquants peuvent coopérer afin de fournir une basse latence pour les communications [25]. Ainsi, quand les attaquants cessent de véhiculer leurs messages, l'état du réseau de capteurs WSN devient instable, et requiert une réinitialisation.

Le renvoi géographique est la défense adéquate, qui résiste à ces attaques, car chaque message est envoyé au capteur le plus proche physiquement. Hu et al [26] décrivent une défense

basée sur les laisses (leashes) des paquets, où la distance de voyage d'un message est limitée, chaque message a un horodatage et une localisation de son émetteur. Le récepteur compare ces informations avec sa propre localisation et horodatage pour vérifier si les intervalles de transmissions sont dépassés.

La figure 3.4 (a et b) montre une situation où une attaque "Wormhole" prend effet. Quand un capteur B (une station de base ou un capteur intermédiaire) envoie un paquet de routage, l'attaquant reçoit ce paquet et le renvoie à ses capteurs voisins Z. Chaque voisin, recevant ce paquet renvoyé, se considère comme voisin du capteur B, et le marque comme son parent. Par conséquent, même si le capteur victime Z est à plusieurs sauts du capteur B, l'attaquant lui transmet l'information qu'il est à un saut seulement du capteur B, créant ainsi un "Wormhole".

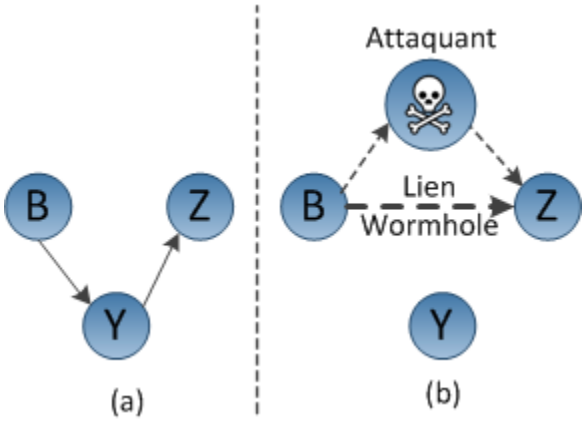

Figure 3.4 L'attaque "Wormhole" [4].

3.6.8 Sybil

Dans plusieurs cas, les capteurs d'un réseau WSN, ont besoin de coopérer afin d'exécuter une tâche. De nouveaux capteurs peuvent prendre l'identité d'autres capteurs légitimes (voir figure 3.5) ce qui définit une attaque "Sybil" [27] qui dégrade l'intégrité des données, leur sécurité, et leurs ressources.

L'attaque "Sybil" s'effectue contre le stockage distribué, le mécanisme de routage, l'agrégation des données, l'élection, l'allocation des ressources, et contre la détection des mauvais comportements "misbehavior detection" [27]. Même si tous les réseaux ad-hoc sont vulnérables aux attaques "Sybil", le réseau de capteurs WSN peut être protégé, en utilisant des protocoles appropriés. Douceur [28] montre qu'en absence d'une autorité centrale, l'attaque "Sybil" peut se réaliser facilement, sauf si de grandes ressources sont utilisées.

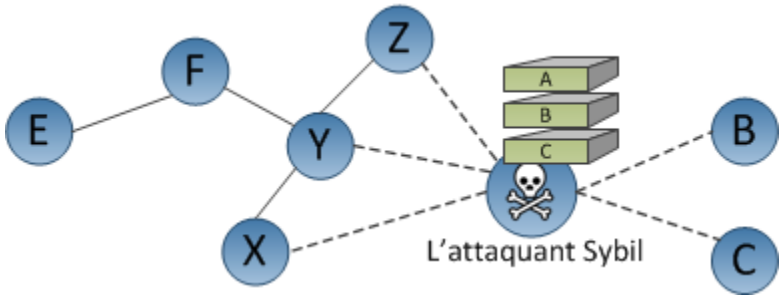

Figure 3.5 L'attaque Sybil [4].

Cependant la détection de l'attaque "Sybil" est difficile, ainsi Newsome et al [29] montrent que celle-ci est très peu probable via des ressources radios. Lors d'une attaque "Sybil", l'attaquant possède de multiples identités et peut se présenter dans plusieurs lieux au même moment, la probabilité de choisir ce faux capteurs est élevée, ce qui entraine une dégradation de la garantie de la qualité fournie par les protocoles multi-saut.

Souvent, les protocoles assument que les capteurs ont une clef unique, et comme l'élément essentiel de l'attaque "Sybil" est la fraude contre l'identité, la propre authentification est la défense principale. Un serveur de clés fiables ou bien une station de base fiable peuvent authentifier un capteur pour les autres capteurs du réseau, cette méthode est utilisée dans le protocole SPINS [30]. Si une clef unique est utilisée, la découverte de cette clef est critique pour tout le réseau.

La vérification de la localisation des capteurs fait partie des techniques de défense contre "Sybil". Sastry et al [31] montrent qu'un protocole simple, utilisant la différence entre le temps "timestamp" de propagation des informations de capteurs, et la vitesse des ondes sonores, permet de bien vérifier l'identité des capteurs. La combinaison des deux défenses : la vérification de l'identité et la vérification de la localisation, peut prévenir des attaques de dénis de service (DoS) tel que "Sybil".

La figure 3.5 montre un attaquant qui prend l'identité de plusieurs autres capteurs légitimes. Dans cette figure, l'attaquant "Sybil" prend l'identité des capteurs A, B et C.

3.6.9 Flooding

L'attaque "Flooding" surconsomme les ressources limitées des capteurs incluant la mémoire, l'énergie, la fréquence, et la capacité de calcul. Dans un réseau homogène, l'attaquant

ayant les mêmes capacités que sa victime, a une force d'attaque limitée. Cependant, si l'attaquant a plus de puissance que ses victimes, l'attaque de "Flooding" devient performante.

Pour combattre la surconsommation des ressources en mémoire, Aura et al [32] décrivent les principes de la gestion de la communication sans connexion "stateless connexion". Une autre méthode utilisée pour contrer cette attaque, est l'utilisation du puzzle côté client "Client puzzles" où le serveur fournit au capteur un puzzle à résoudre, avec une complexité qui dépend du niveau de la fiabilité du capteur.

3.6.10 Jamming

L'attaque la plus connue des réseaux de capteurs sans fil est le "Jamming", qui interfère avec les fréquences radios du réseau. Un adversaire peut perturber le réseau, en utilisant k capteurs de "Jamming" qui mettent N capteurs hors de service avec $k < N$. Dans un réseau à fréquence unique, cette attaque est simple et efficace.

Les capteurs, disposant de plus de ressources, peuvent déclarer du "Jamming" à la station de base. Wenyuan Xu et al [33] développent un mécanisme de détection des attaques de "Jamming" dans un réseau WSN en les classant en quatre types : constant, trompeur, aléatoire et réactif :

- Le "Jamming" constant corrompt les paquets en transmission dans le réseau WSN, mais en contre partie, l'attaquant doit avoir plus de ressources que ses victimes.
- Le "Jamming" trompeur envoie une trame constante dans le réseau, par exemple dans tinyOS, le dispositif reçoit des bits constants, ce qui oblige les capteurs du réseau à rester en mode réception, ainsi ils ne peuvent plus renvoyer des données sur le réseau.
- Le "Jamming" aléatoire alterne entre l'état de veille et l'état de "Jamming", afin d'économiser de l'énergie.
- Le "Jamming" réactif transmet seulement un signal de "Jamming" en cas de détection d'un signal sur le réseau, mais l'identification du "Jamming" réactif est difficile car il peut être remarqué comme un paquet en collision. Les techniques d'identification des attaques de "Jamming" incorporent des analyses statistiques, concernant les indicateurs de la force des signaux reçus (RSSI), du temps moyen pour capter un canal inoccupé, et du ratio de livraison des paquets (PDR) [1]. Ces trois mesures peuvent être réalisées au niveau de la station de base.

La défense standard est l'utilisation de plusieurs spectres de diffusion. Les capteurs du réseau doivent définir une stratégie [22] pour combattre les brouilleurs, en alternant entre le

sommeil et le réveil, afin de s'échapper des capteurs verrouilleurs.

3.6.11 Tampering

L'attaque de "Tampering" est une attaque de la couche physique dans les réseaux de capteurs sans fil WSN, elle peut être active ou passive. Un attaquant peut endommager ou remplacer un capteur, son matériel de calcul, et ses clés cryptographiques.

La protection contre l'attaque "Tampering" active peut se réaliser avec les circuits physiques, alors que la défense contre l'attaque "Tampering" passive est réalisée à l'aide des technologies intégrées aux circuits matériels.

En pratique, il est impossible de contrôler l'accès aux capteurs dispersés sur plusieurs distances, mais une défense réussie contre cette attaque "Tampering" dépend de plusieurs critères : le niveau de considération des menaces d'attaques lors de la phase de conception, du taux de disponibilité des ressources en phase de la conception, en phase de la construction et en phase de test, et enfin du taux de détermination de l'attaquant.

La défense contre les capteurs internes corrompus et les capteurs passants intelligents est relativement simple, en comparaison avec les capteurs ayant de grandes ressources. Le camouflage des paquets, la dissimulation des capteurs, et l'utilisation des techniques de probabilités faibles d'interception des radios (LPI), sont des techniques de sécurité contre l'attaque de "Tampering" [3]. Cependant, ces techniques augmentent le coût et la complexité, de la conception de réseaux de capteurs sans fil WSN.

3.6.12 Unfairness

L'attaque de "Unfairness" ne peut pas empêcher totalement l'accès légitime à un canal, mais elle peut dégrader ce service en causant, par exemple, une augmentation des délais des protocoles MAC utilisées.

Pour se défendre contre cette attaque, il est utile d'utiliser des cadres d'informations de petites tailles "Small frames" ainsi un capteur ne peut capturer un canal que pour une courte durée.

3.6.13 Attaque de Collisions

Un adversaire a besoin d'introduire une collision dans un seul octet d'un paquet en transmission, pour le perturber en entier. Une modification dans une portion de données, peut

causer une erreur de vérification au niveau du récepteur. Dans ce cas, l'attaquant a besoin d'une quantité minime d'énergie.

Le réseau peut utiliser des mécanismes de détection de collisions, pour identifier les collisions malveillantes créant un "Jamming" de la couche liaison, mais aucune défense effective n'est connue.

La détection de la collision est difficile, car l'attaquant ignore tout simplement les protocoles de protection. Le codage de correction d'erreurs peut être utilisé contre la corruption des données, cependant l'attaquant peut corrompre plus de données que le codage ne peut corriger [22].

3.6.14 Exhaustion and Interrogation

Cette attaque compromet la disponibilité du réseau. Le multiplexage en division temporelle, donne à chaque capteur un intervalle de temps pour la transmission sans arbitrer entre les "frames".

Une des solutions est la limitation du taux de transmission, ainsi le réseau ignore les transmissions expansives. Un attaquant peut effectuer un déni de service à un réseau de capteurs WSN, en introduisant des retransmissions suite à une corruption d'une petite partie d'un message. La défense contre cette attaque peut être l'authentification des requêtes [22].

3.6.15 Attaque de désynchronisation

Une connexion existante entre deux points peut être perturbée par la désynchronisation. Lors de cette attaque, l'adversaire envoie de manière répétitive des messages à l'une des deux extrémités de la connexion, et provoque la retransmission des données.

Pour se défendre de cette attaque, il est possible d'authentifier les paquets, et leurs champs de contrôle dans l'entête [34].

3.6.16 Attaque "HELLO flood"

L'attaque "Hello flood" est effectuée par un attaquant disposant de grandes ressources, qui envoie des messages "HELLO" à un grand nombre de capteurs, dans une large région de réseau de capteurs sans fil WSN. Ainsi, les capteurs victimes croient que les adversaires sont leurs voisins, et leurs envoient des messages qui devraient aboutir à la station de base.

Pour se défendre contre cette attaque, il est possible d'utiliser le mécanisme d'authentification par un capteur tier [1].

3.6.17 Algorithmic complexity

Le succès de l'attaque "algorithmic complexity" dépend de plusieurs éléments. Un service attaqué doit utiliser un algorithme et une structure de données telle qu'une table de hachage. Les entrées de l'algorithme doivent être contrôlées par l'attaquant, afin de compromettre leurs valeurs, ensuite ces données sont envoyées à un capteur victime, qui dépensera beaucoup de temps et de ressources pour traiter ces données reçues.

Pour se défendre contre cette attaque, il est utile de limiter la taille des structures de données [35].

3.7 Conclusion

Plusieurs types d'attaque existent et pour chacune d'elles, une stratégie de défense est définie (voir tableau 3.1).

L'autocorrection dans un réseau de capteur sans fil WSN, rend le travail de l'attaquant plus difficile. Selon une étude de "NIST's ICAT vulnerability search engine", il existe depuis 2002, plus de 335 codes sur le web utilisables à distance, pour exploiter les vulnérabilités des réseaux de capteurs WSN.

Dans le chapitre suivant, nous décrivons l'attaque d'analyse de trafic, et certaines défenses contre cette attaque.

CHAPITRE 4

ATTAQUE D'ANALYSE DE TRAFIC ET DEFENSES

4.1 Introduction

L'attaque d'analyse de trafic est une attaque passive, qui reconnaît le patron (pattern) du trafic du réseau de capteurs sans fil WSN, en analysant les mouvements des paquets dans le réseau. Ensuite, cette attaque déduit la localisation des capteurs stratégiques, et effectue une attaque de déni de service.

La défense contre l'attaque d'analyse de trafic réside dans la prévention contre cette découverte de localisation. Les traditionnelles méthodes d'encryptage des données ne sont pas efficaces contre l'attaque d'analyse de trafic, car ces méthodes permettent seulement de cacher le contenu des données, et non la localisation de la station de base.

Plusieurs techniques sont développées pour contrer ce type d'attaque [36], par exemple :

- « Random Routing Scheme » (RRS) pour diversifier les routes des messages.
- « Dummy Packet Injection Scheme » (DPIS) pour confondre l'attaquant par injection de faux paquets.
- « Anonymous Communication Scheme » (ACS) qui cache l'identité des capteurs participant à une communication.

Un réseau de capteurs sans fil WSN est un réseau de distribution de capteurs autonomes, capables de détecter et réagir à des événements divers dans leurs environnements. Des menaces contre les réseaux de capteurs WSN, comme l'attaque d'analyse de trafic, devient un élément important à prendre en compte pour le bon fonctionnement d'un réseau de capteurs sans fil WSN. L'attaquant peut déduire les stations de base du réseau en observant les volumes de trafic et leurs formes (patterns). Ainsi, il peut effectuer une attaque de déni de service contre les capteurs stratégiques du réseau, créant une paralysie dans le réseau. La manière optimale de défense de la station de base contre l'attaque d'analyse de trafic est la modification de l'allure générale du trafic dans le réseau, en créant de nouvelles régions ayant un trafic volumineux.

La figure 4.1 montre le trafic au niveau de chaque capteur en utilisant le schéma SP « short path scheme», qui détermine le chemin le plus court pour l'envoi des données à partir d'un

capteur vers la station de base. Les capteurs, voisins de la station de base, renvoient plus de trafic que les autres capteurs. En visualisant ce trafic, un attaquant peut déduire la région de la station de base. Par exemple :

- Si le contenu du message est un « texte simple» qui ne contient que des données, l'adversaire peut déterminer les paquets qui sont envoyés vers la station de base. Ce qui permet à l'attaquant de suivre la direction de ces paquets pour trouver la station de base.
- S'il existe une corrélation temporelle entre la réception d'un paquet par un capteur, et son renvoi, l'attaquant peut identifier ce paquet et le suivre saut par saut, jusqu'à la station de base.
- Comme la communication est élevée au voisinage de la station de base, un adversaire peut localiser cette dernière en suivant les régions de trafic élevé.

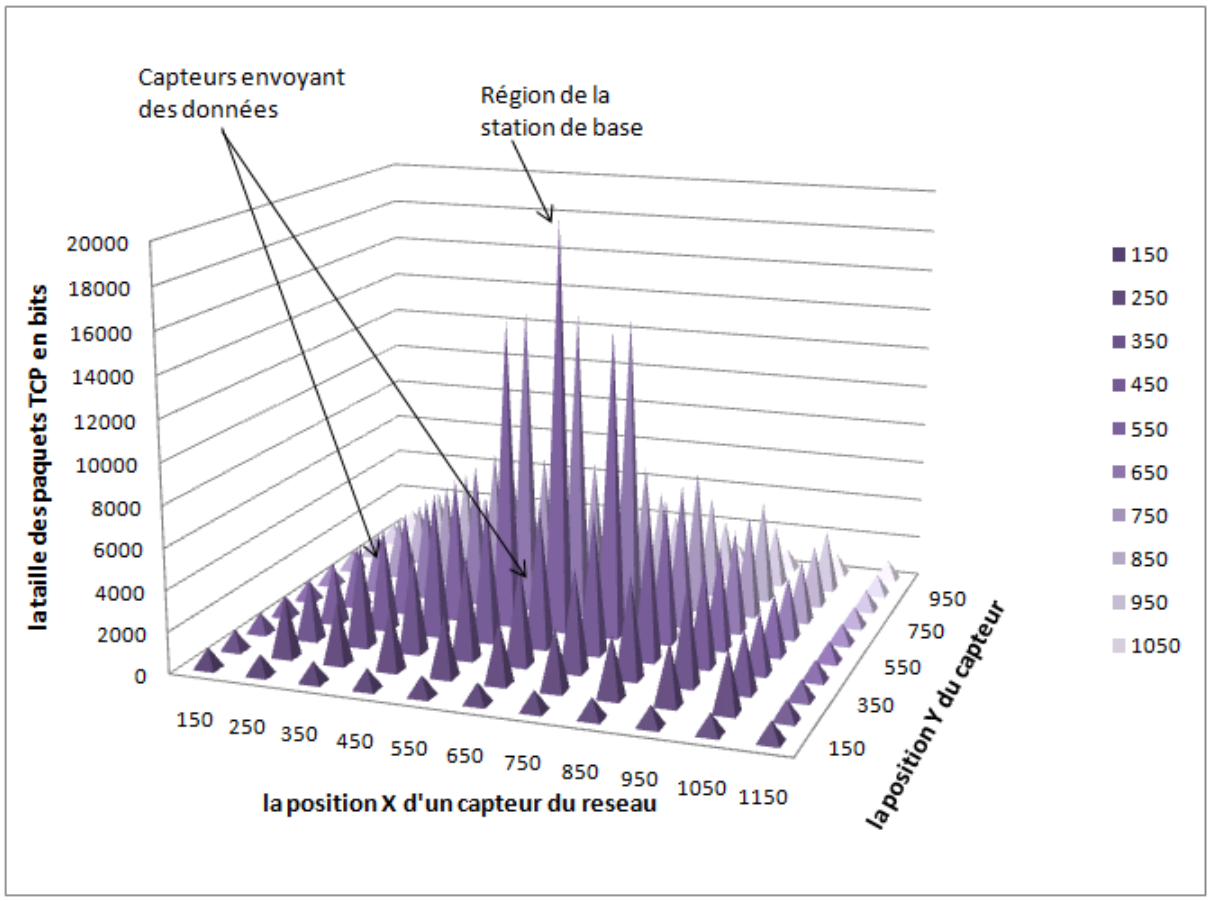

Figure 4.1 Un graphe 3D du trafic des données dans un réseau de capteurs sans fil WSN [5].

4.2 Description de l'attaque d'analyse de trafic

En général, un adversaire peut effectuer cette attaque de trois manières :

- L'attaque par observation de taux « Rate Monitoring Attack » [5] [37] est basée sur le fait que les capteurs voisins de la station de base, envoient plus de messages que les capteurs éloignés de la station de base. Ainsi, un adversaire comptabilise le taux d'envoi des paquets, afin de connaître les capteurs qui envoient le plus de paquets.
- L'attaque par corrélation temporelle « Time Correlation Attack » (appelée aussi l'attaque de traçage des paquets « packet tracing attack ») où l'attaquant calcule le temps d'envoi des paquets corrélés au travers des capteurs voisins, et essaye de tracer l'émission des paquets jusqu'à la station de base, ainsi l'attaquant suit un paquet à chaque saut jusqu'à la station de base.
- L'attaque d'analyse des identifiants (ID), où un adversaire tente de détecter les relations entre les communications des capteurs, et ensuite en déduire le patron (pattern) du trafic en vérifiant les identités des paquets.

4.3 Défense contre l'attaque d'analyse de trafic

Il y a plusieurs approches de défense contre l'attaque d'analyse de trafic, mais ces méthodes ne permettent pas une défense optimale, car elles consomment beaucoup d'énergie. Dans ce sens, Deng et al. [5] se concentrent sur les techniques de dissimulation de la localisation de la station de base contre l'attaque du taux de trafic. À cette fin, ils utilisent trois techniques :

- Les routes multi-saut des paquets en transmission, sont choisies avec un certain degré d'aléatoire.
- Certaines routes munies de faux paquets sont ajoutées dans le réseau.
- Plusieurs régions ayant un important faux trafic sont créées dans le réseau.

Cependant, ces techniques demeurent inefficaces contre l'attaque de corrélation temporelle. Jing Deng et al. [38] évaluent des contres mesures pour cacher la localisation de la station de base contre l'attaque d'analyse de trafic tels :

- Le ré-encryptage des paquets à chaque saut pour changer leur apparence.
- La désignation d'un taux d'envoi de paquets uniforme.
- La suppression de la corrélation entre le temps de réception des paquets, et le temps de renvoi.

Jing Deng et al. [38] créent de multiples régions appelées « hot spots », dont ils démontrent l'efficacité analytiquement et par simulation en utilisant trois critères de mesure d'évaluation :

- L'entropie totale du réseau.
- L'énergie totale consommée du réseau.
- Le comportement de l'attaquant face aux contres mesures.

Par ailleurs, Ying et al. [37] proposent une défense contre l'attaque de corrélation temporelle appelée aussi attaque de traçage de paquets, en créant un trafic de données uniformément distribué dans tout le réseau de capteurs sans fil WSN.

Afin de protéger la station de base, Xi Luo et al. [39] présentent une technique contre les trois types d'attaque d'analyse de trafic. Pour contrer l'attaque de surveillance du taux, ils choisissent aléatoirement un des capteurs voisins pour renvoyer les messages qui sont plus proches du capteur récepteur, afin de diminuer le temps de latence de transmission. Ils introduisent des faux paquets «dummy packet» qui sont ajoutés au trafic pour créer de la diversion, et enfin, ils utilisent des mécanismes d'anonymat pour cacher l'identité des capteurs qui participent à la transmission des paquets. Ils utilisent un réseau d'une centaine de capteurs, et considèrent un attaquant de type «localization evesdropper» qui détecte les transmissions par triangulation, et réside auprès d'une région afin de compter les paquets en transition. Ils proposent les deux techniques suivantes :

1. La technique RRS «Random Routing Scheme» qui permet aux capteurs d'envoyer des paquets dans des directions différentes. Afin de calculer la probabilité d'envoi d'un paquet vers un capteur, ils divisent les voisins d'un capteur en deux groupes dépendamment du nombre n de sauts de la station de base :
   - Le groupe des voisins à moins de n.
   - Le groupe des voisins à plus de n.
2. La technique «Dummy packet injection Scheme» (DPIS) [39] pour défendre une station de base contre l'attaque de surveillance par taux de paquets «Packet Rate Monitoring Attack», couplée à l'attaque de traçage de paquets «Packet Tracing Attack». Avec la technique DPIS, les faux paquets sont injectés avec une certaine probabilité proportionnelle à l'énergie résiduelle des capteurs.

Jian et al. [37] proposent une technique «Location Privacy Routing Protocol» (LPR) qui défend la station de base seulement contre l'attaque de traçage de paquets. Ils combinent la diversification des routes avec l'injection de faux paquets, en utilisant un paramètre de probabilité de génération de faux paquets par un capteur réacheminant un vrai paquet.

4.4 Conclusion

Au cours de ce chapitre, nous avons décrit l'attaque d'analyse de trafic et les défenses possibles contre cette attaque, mettant en place de nouvelles routes et générant du faux trafic.

Dans le chapitre suivant, nous présentons le simulateur J-Sim pour mettre en place les caractéristiques du réseau de capteurs de notre nouvelle technique de défense contre l'attaque d'analyse de trafic, en utilisant une fausse station de base ***mobile***.

CHAPITRE 5

LA SIMULATION AVEC L'OUTIL J-SIM

5.1 Introduction

Dans ce mémoire, nous utilisons une nouvelle technique de défense d'un réseau de capteurs WSN contre l'attaque d'analyse de trafic, par l'introduction d'une fausse station de base mobile dans le réseau WSN. Nous testons cette nouvelle technique à l'aide de l'outil J-Sim. Cet outil a l'avantage de permettre une simulation des réseaux WSN munis d'un grand nombre de capteurs sans fil, et cela sans dépassement de mémoire.

Au cours de ce chapitre, nous décrivons la configuration du réseau de capteurs WSN simulé et son architecture.

5.2 La configuration du réseau simulé

Notre étude propose une nouvelle approche de protection d'un réseau de capteurs sans fil WSN contre l'attaque de l'analyse de trafic. Nous traitons d'un réseau étendu sur une zone de 1500×1500 unités. Nous avons utilisé une centaine de capteurs intermédiaires, deux capteurs émetteurs "Target", et une station de base.

La première étape de notre technique proposée, est la définition des positions des cent capteurs intermédiaires dans la topologie du réseau, les positions de la station de base, et les deux "Target". La deuxième étape consiste à comptabiliser le trafic dans le réseau simulé.

Dans notre étude, le réseau de capteurs WSN a une densité de 100 capteurs (pouvant être mobiles), qui communiquent entre eux avec la fréquence libre de 916 MHZ. Le réseau de capteurs WSN envoie les données des capteurs vers la station de base qui dispose de grandes ressources énergétique et de calcul.

En général, les capteurs de réseaux WSN sont déployés d'une manière ad-hoc, mais notre étude déploie ces capteurs uniformément sur une grille de 1500×1500 unités, afin de mieux maîtriser les communications entre eux. La matrice des positions des capteurs est définie dans le tableau 5.1. La station de base est numérotée "0", les capteurs intermédiaires sont numérotés de 1 à 100, et les deux capteurs "Target" sont numérotés "101" et "102". Ainsi, la

matrice du tableau 5.1 montre les positions des 103 capteurs numérotés de 0 à 102. Donc selon le tableau 5.1, le capteur 2 est positionné dans la zone X [400, 500] et Y [500, 600].

Tableau 5.1 Les positions des capteurs dans le réseau étudié WSN

	100-200	200-300	300-400	400-500	500-600	600-700	700-800	800-900	900-1000	1000-1100
100-200	82 et 101	54	53	52	51	50	81	80	79	78
200-300	83	55	29	28	27	26	49	48	47	77
300-400	84	56	30	11	10	9	25	24	46	76
400-500	85	57	31	12	2	1	8	22 et 23	45	75
500-600	86	58	32	13	3	0	7	21	44	74
600-700	87	59	33	14	4	5	6	20	43	73
700-800	88	60	34	15	16	17	18	19	42	72
800-900	89	61	35	36	37	38	39	40	41	71
900-1000	90	62	63	64	65	66	67	68	69	70
1000-1100	91	92	93	94	95	96	97	98	99	100 et 102

Lors de notre étude, chacun des deux capteurs ”Target” envoie des données aux capteurs, ensuite ces capteurs envoient ces messages à la station de base où les données sont encapsulées, en utilisant les communications multi-saut.

Le protocole utilisé dans les capteurs est AODV. Celui-ci met à jour les tables de routage au niveau de chaque capteur. Cette mise à jour induit du trafic AODV dans le réseau de capteurs WSN. Aussi, chaque capteur est capable d'injecter des paquets TCP dans le réseau WSN en définissant le capteur destinataire de ces paquets.

Après l'installation des différents capteurs du réseau WSN simulé, une simulation de 100 secondes est démarrée, et l'affichage des données est rafraichit chaque seconde. Le trafic est généré initialement par des ”Targets” qui envoient des stimuli fixes chaque demi-seconde. Ensuite, les sources TCP des capteurs intermédiaires génèrent des messages TCP chaque demi-seconde, et ayant pour destination finale la station de base numérotée ”0”.

5.3 L'architecture du réseau simulé

Le simulateur J-Sim est composé de deux canaux de communications (voir la figure 5.1) : le canal sans fil "Wireless Channel", et le canal de capture "Sensor Channel".

Le réseau d'évaluation est aussi composé de trois types de capteurs : (i) capteur "Target", (ii) capteur "station de base", et (iii) capteur "intermédiaire". Les capteurs "intermédiaires" et "la station de base" communiquent via le canal sans fil, alors que les capteurs "Target" et les capteurs "intermédiaires" communiquent entre eux via le canal de capture.

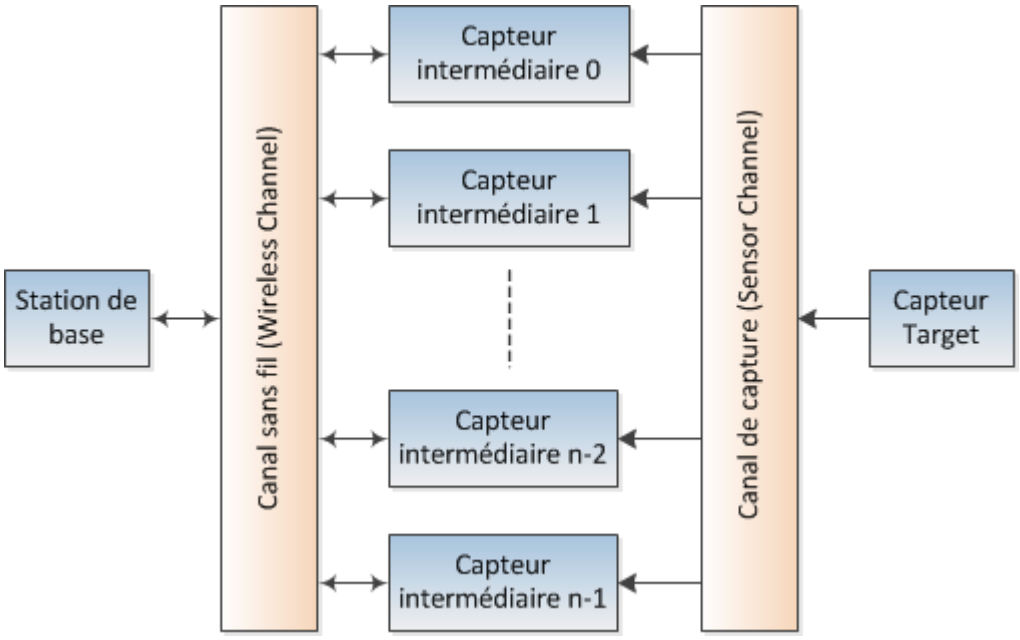

Figure 5.1 Les communications entre les capteurs du réseau WSN via le canal de capture "Sensor channel" et le canal sans fil "Wireless channel" [6].

5.3.1 Les communications entre les capteurs du réseau WSN

La figure 5.1 montre que les deux capteurs "Targets" envoient leurs stimuli au canal de capture, et que les capteurs intermédiaires "sensor nodes" lisent leurs informations du canal de capture "Sensor Channel", puis les renvoient au canal sans fil "Wireless Channel". Le capteur "station de base" lit et écrit des informations au niveau du canal sans fil "Wireless Channel".

5.3.2 Les couches du capteur station de base

La figure 5.2 montre les couches du capteur ”station de base” communiquant entre elles, afin de collecter les informations du canal sans fil ”Wireless channel”.

Les informations circulent dans les deux sens entre les différentes couches (voir la figure 5.2) dans l'ordre suivant :

1. La couche physique recevant les informations du canal sans fil, ou de la couche MAC ;
2. La couche MAC située entre la couche physique et la couche réseau, et qui échange les informations entre les deux couches ;
3. La couche réseau située entre la couche MAC et la couche transport, et qui échange les informations entre les deux couches ;
4. Puis, la couche transport située entre la couche réseau et la couche application, et qui échange les informations entre les deux couches ;
5. Et finalement, la couche application, qui échange les informations avec la couche transport.

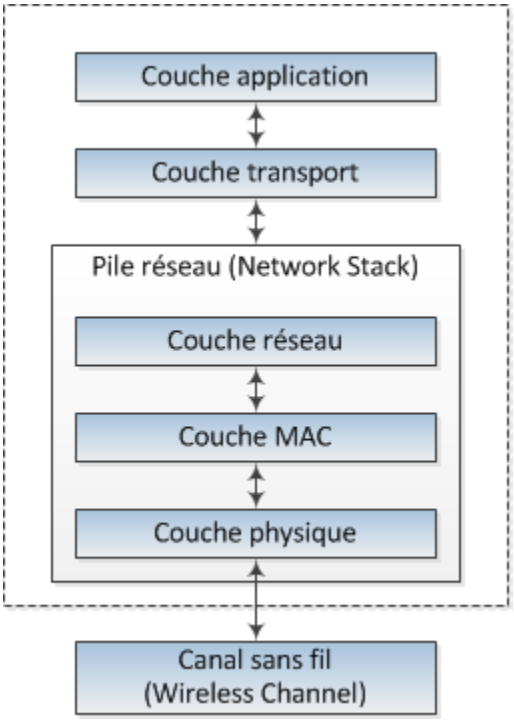

Figure 5.2 Les couches d'un capteur ”station de base” communiquant avec le canal sans fil ”Wireless Channel” [6].

5.3.3 Les couches du capteur ”Target”

La figure 5.3 montre les couches du capteur ”Target” qui communiquent entre elles, afin d'envoyer les informations au canal de capture ”Sensor channel”.

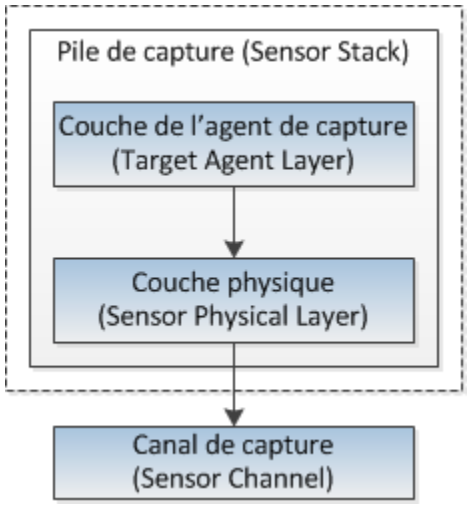

Figure 5.3 Les couches du capteur ”Target” communiquant avec le canal de capture ”Sensor Channel” [6].

5.3.4 Les couches du capteur intermédiaire

La figure 5.4 montre les couches du capteur intermédiaire, qui lit les stimuli des ”Targets” via le canal de capture. Ce capteur reçoit et envoie des données, via le canal sans fil vers la station de base, et aux autres capteurs intermédiaires. Ces derniers consomment l'énergie de leurs batteries, pour traiter des données via ”CPU Model”, ou les capturer via ”radio Model”.

Les différentes couches du capteurs intermédiaires sont (voir la figure 5.4) :

- La couche physique de capture ”Sensor Physical layer”, lisant les données du canal de capture. Ces données sont ensuite envoyées à la couche de l'agent de capture ”Target Agent layer” ;
- La couche de l'agent de capture ”Target Agent Layer”, qui envoie les données reçues à la couche d'application ;
- La couche application, qui communique directement avec la couche transport ;
- La couche transport, qui envoie et reçoit des données de la couche réseau ;
- La couche réseau communiquant avec la couche MAC ;
- Et enfin, la couche physique, qui renvoie les données vers le canal sans fil.

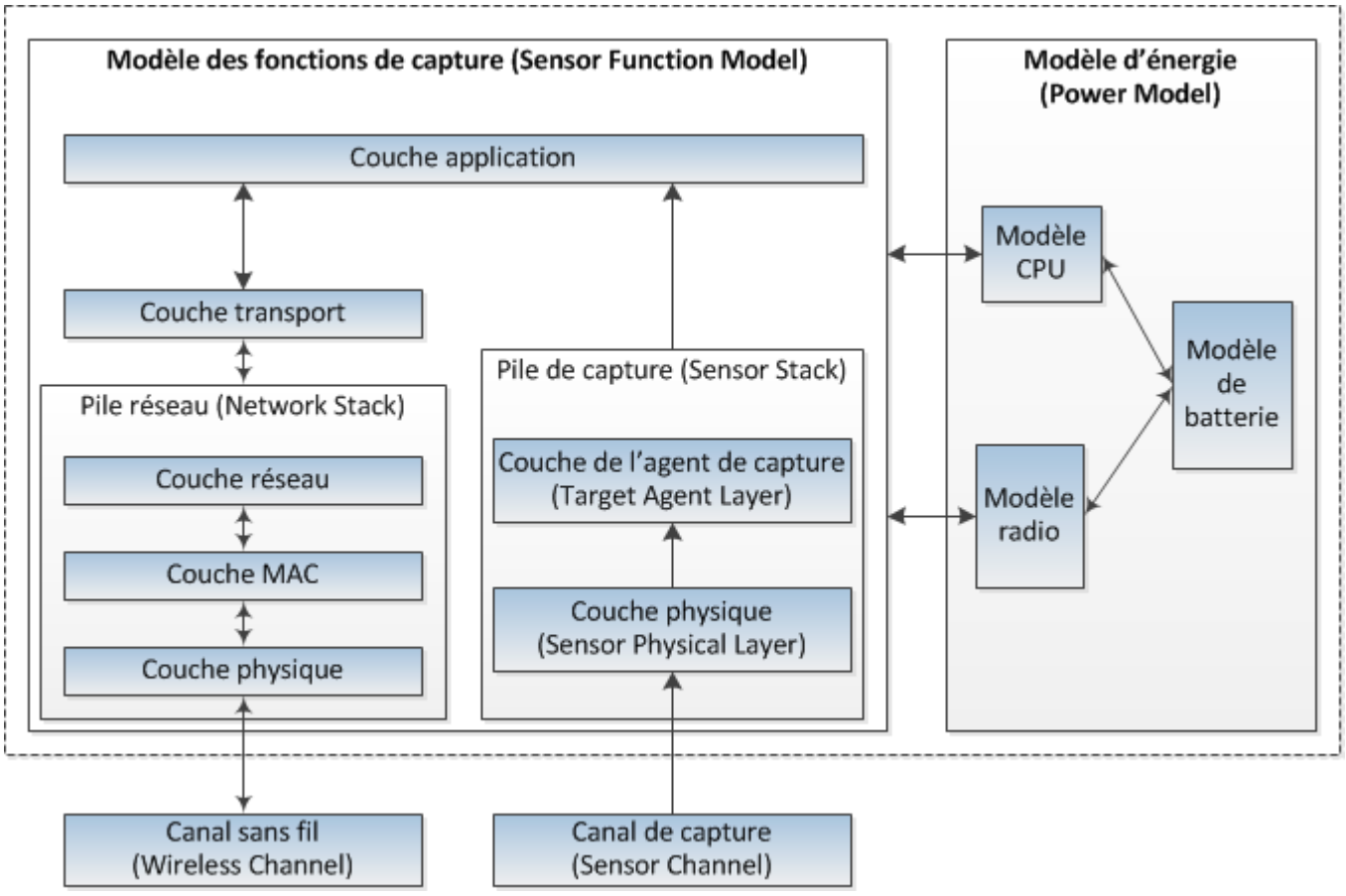

Figure 5.4 Les couches du capteur "intermédiaire" lisant les stimuli du canal de capture, et communiquant avec les autres capteurs via le canal sans fil [6].

5.3.5 L'architecture du capteur "Target"

Le capteur "Target" (figure 5.5) génère toutes les demi-secondes des stimuli, qui sont propagés dans le canal de captage "Sensor Channel". Ces stimuli sont ensuite capturés par les capteurs voisins.

La figure 5.5 montre la composition du capteur "Target", qui est constitué des sous-composants suivants :

- L'agent de capture "Target Agent",
- La couche physique "Sensor Phy",
- Et le modèle de mobilité "Sensor Mobility Model".

L'agent de capture "Target Agent" génère des stimuli, et les envoie à la couche physique "Sensor Phy", qui à son tour les envoie au canal de capture "Sensor Channel". Le modèle de

mobilité "Sensor Mobility Model" est responsable du positionnement de son capteur dans la topologie du réseau.

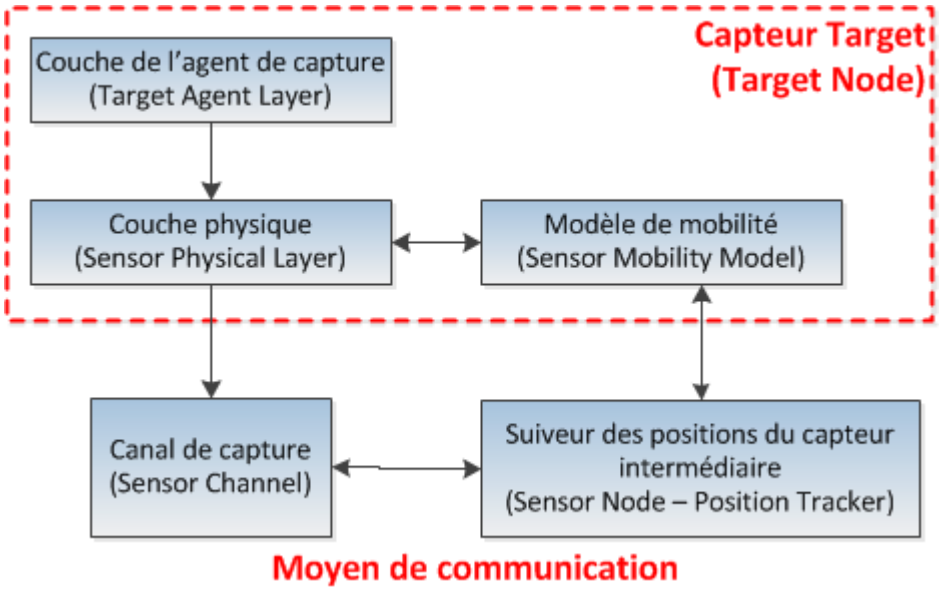

Figure 5.5 L'architecture du capteur "Target" de J-Sim [6].

5.3.6 L'architecture du capteur station de base

La station de base (voir la figure 5.6) reçoit des informations propagées dans le canal sans fil "Wireless Channel". Ces informations sont envoyées et répercutées par des capteurs intermédiaires voisins. La figure 5.6 montre les sous-composants de la station de base :

- L'agent de mobilité "Mobility Model", qui est responsable de la localisation et du déplacement de la station de base.
- La couche physique "Wireless Phy", qui permet d'envoyer et recevoir des messages du canal sans fil "Wireless Channel".
- Le composant de routage "Ad Hoc routing", qui implémente le routage AODV de notre étude.
- Le sous composant de propagation sans fil "Wireless Propagation Model", contenant les informations nécessaires pour propager les informations d'un capteur à un autre.
- Le sous composant "TCP Sink", qui est ajouté à la station de base afin de recevoir les messages TCP envoyés par les capteurs intermédiaires.
- Le sous composant MAC, qui utilise le standard "MAC 802.11".
- La couche IP "PktDispacher", qui renvoie les paquets reçus vers les autres couches du capteur.

– Le sous-composant de propagation sans fil ”Wireless Propagation Model”, qui implémente le modèle de propagation.
– Le sous-composant ”RT”, qui gère la table de routage.

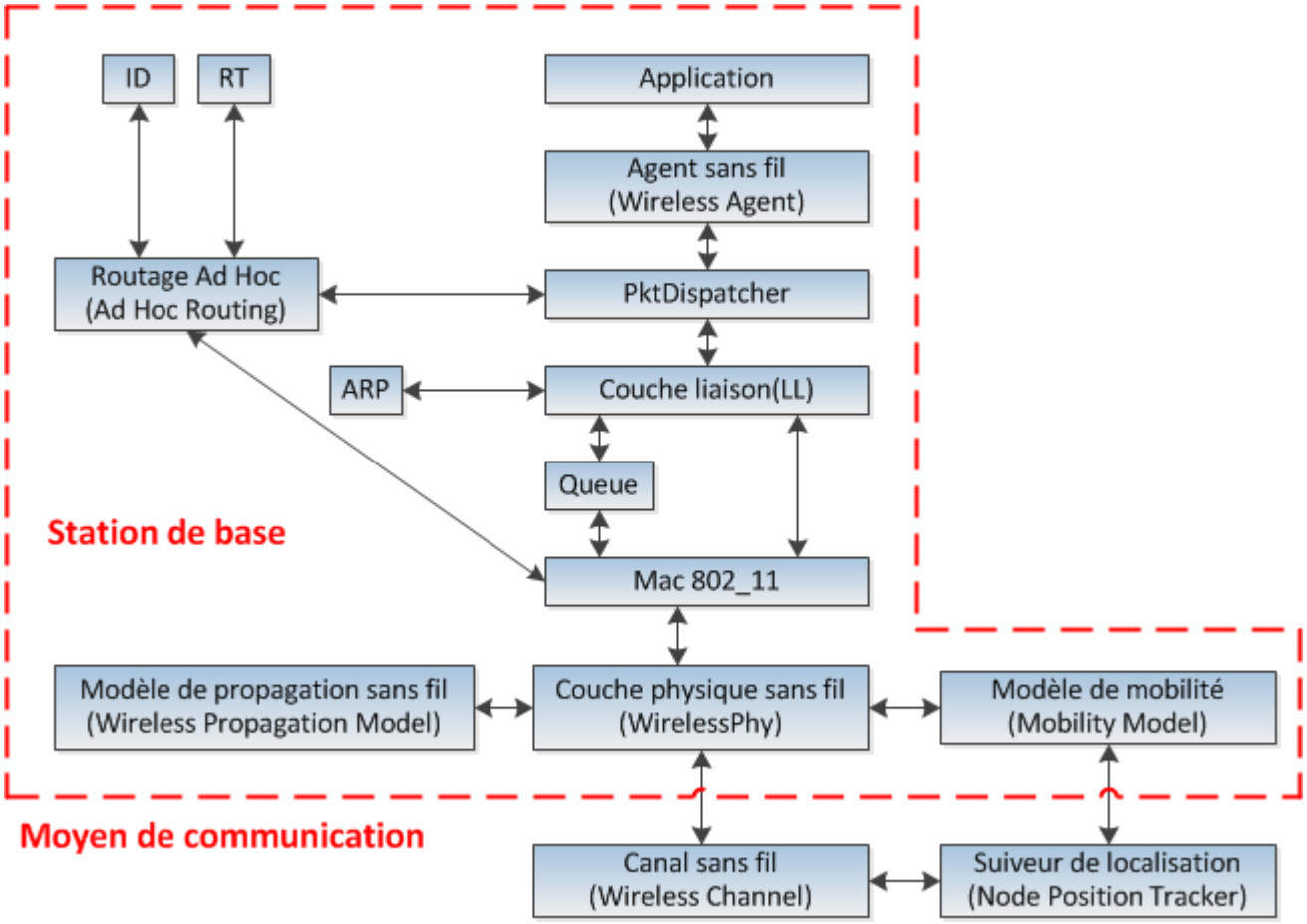

Figure 5.6 L'architecture du capteur ”station de base” de J-Sim [6].

5.3.7 L'architecture du capteur intermédiaire

Le capteur intermédiaire (voir la figure 5.7) reçoit des stimuli, qui se propagent dans le canal sans fil ”wireless Channel”, et d'autres stimuli, qui s'injectent dans le canal sans fil ”Wireless Channel” par des capteurs voisins.

Le capteur intermédiaire reçoit aussi les informations, envoyées par les capteurs ”Targets” voisins, et propagées dans le canal de capture ”Sensor Channel”. Toutes ces informations sont ensuite envoyées à la station de base, et aux capteurs intermédiaires voisins.

La figure 5.7 montre les sous composants suivants d'un capteur intermédiaire :

- Le composant physique "Wireless Phy", qui est responsable de l'écriture et de la lecture à partir du canal sans fil "Wireless Channel".
- Le composant de routage ad-hoc "Ad hoc Routing" contenant les informations du routage AODV.
- Le modèle de mobilité "Sensor Mobility Model" responsable de la localisation, et du déplacement d'un capteur intermédiaire.
- L'évier des paquets TCP "TCP Sink" ajouté au capteur intermédiaire (qui devient une fausse station de base), afin de recevoir les messages TCP envoyés par d'autres capteurs intermédiaires.
- La source TCP "TCP Source" additionnée au capteur intermédiaire, pour lui permettre d'être une source de messages TCP.

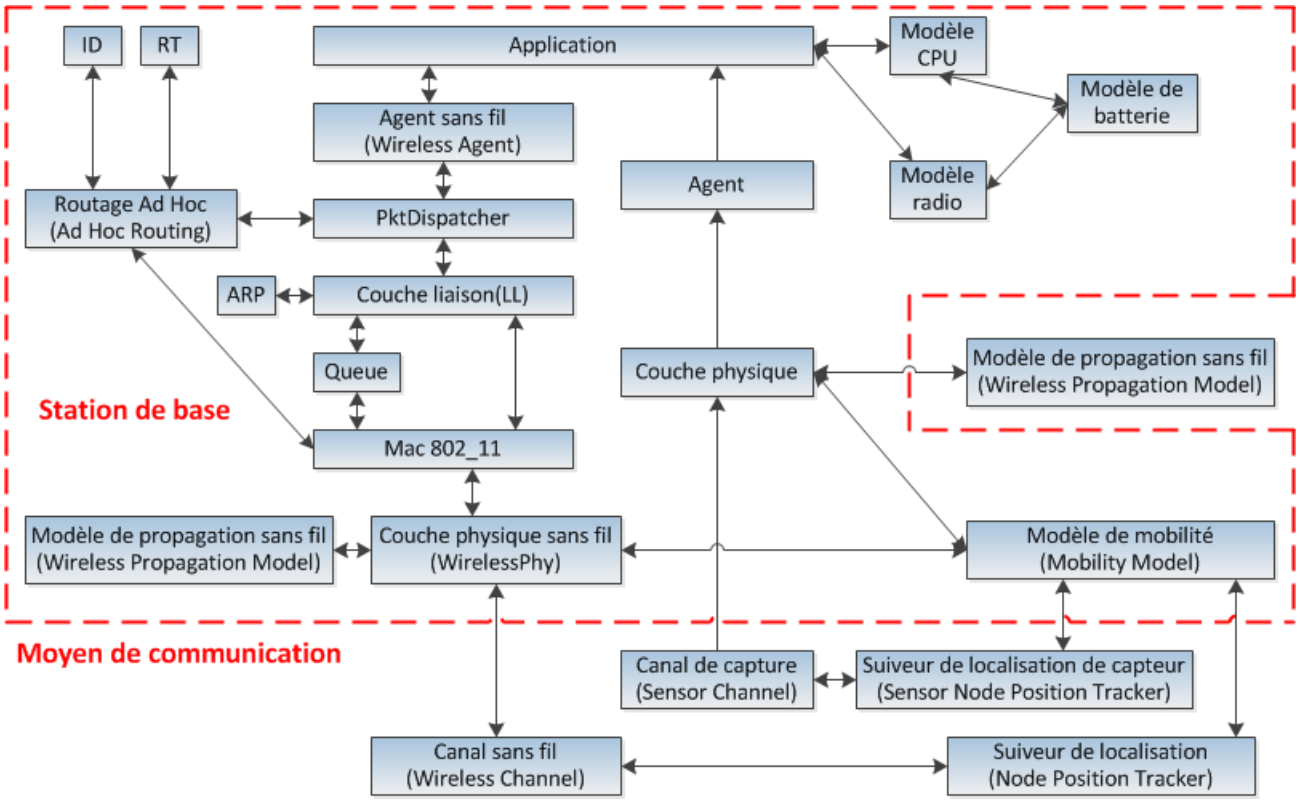

Figure 5.7 L'architecture du capteur intermédiaire de J-Sim [6].

5.4 Conclusion

Au cours de ce chapitre, nous avons détaillé l'architecture des différents intervenants du simulateur : capteurs, "Targets", station de base. La description des architectures permet de détailler le rôle des intervenants.

Pour tester la défense contre l'attaque d'analyse de trafic, nous utiliserons une technique novice par l'introduction d'une fausse station de base ***mobile***. Cette nouvelle technique est détaillée dans le chapitre suivant.

CHAPITRE 6

PROPOSITION D'UNE TECHNIQUE DE PROTECTION CONTRE L'ATTAQUE D'ANALYSE DE TRAFIC DANS UN RÉSEAU DE CAPTEURS WSN

6.1 Introduction

Suite à la configuration et l'installation des différents capteurs du réseau WSN, à simuler pour une durée de 100 secondes, le trafic du réseau de capteurs sans fil WSN fonctionne correctement, et les messages TCP transitent normalement, entre les différents capteurs intermédiaires et la station de base. De même, les trafics des paquets AODV et des stimuli des "Targets" sont bien acheminés entre les différents composants du réseau WSN de notre simulation. Des figures seront tracées pour donner un aperçu de la fluidité des communications du réseau de capteurs WSN et pour valider notre technique.

6.2 Le cheminement de la technique de protection

Notre nouvelle technique de protection contre l'attaque de l'analyse de trafic, se base successivement sur les éléments ci-dessous :

1. La simulation d'un réseau WSN constitué de $n = 100$ capteurs, $m = 1$ station de base et $t = 2$ "Targets".
2. Les "Targets" génèrent des stimuli à destination de la station de base.
3. Un trafic TCP est généré par l'ensemble des n capteurs à destination des stations de base.
4. Un trafic AODV est généré par le réseau simulé, afin de trouver les routes des capteurs vers la station de base.
5. Les patrons (patterns) des trafics sont vérifiées, pour valider le bon cheminement des données dans le réseau WSN.
6. Ensuite, un paramètre h nombre de sauts de la station de base est choisi. Une période T est choisie afin de déplacer la fausse station de base chaque T secondes.
7. s capteurs générant du faux trafic TCP sont élus, et une fausse station de base est élue pour recevoir ce faux trafic. Les s capteurs collaborateurs et la fausse station de base, sont à au moins h sauts de la vraie station de base.

8. Suite à la génération de faux trafic, les patrons (patterns) des trafics dans le réseau WSN simulé sont vérifiés, afin de conclure que la région de la fausse station de base a le volume le plus important du réseau.
9. Cette région de la fausse station de base est mobile, car la fausse station de base se déplace chaque T secondes.

Notre nouvelle technique est implémentée via un script TCL qui s'exécute selon les étapes décrites dans la figure 6.1.

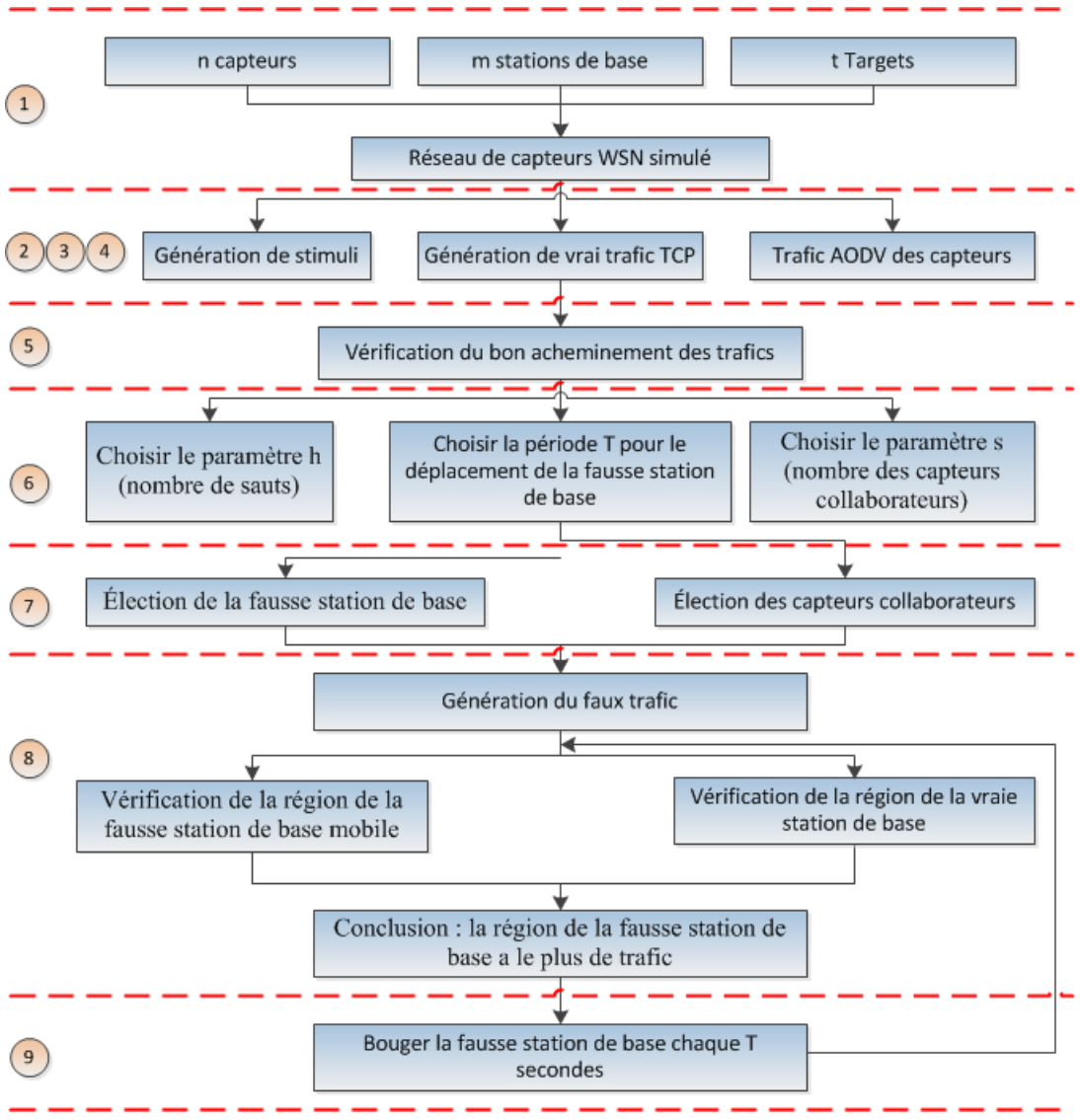

Figure 6.1 Description des étapes du script TCL de la nouvelle technique de protection contre l'attaque d'analyse de trafic

6.3 La présentation des trafics dans le réseau simulé

Lors de cette section, nous analysons les trafics des stimuli, des paquets TCP et AODV au niveau de la station de base, et des capteurs du réseau WSN simulé.

6.3.1 Le trafic des stimuli dans le réseau simulé

La figure 6.2 a pour coordonnées (en x-abscisse) le temps de simulation, et (en y-ordonnée) la quantité en bits des stimuli des deux "Targets" reçus par la station de base. Cette figure montre que les stimuli des "Targets" sont bien reçus par la station de base, ce qui signifie que le réseau fonctionne correctement.

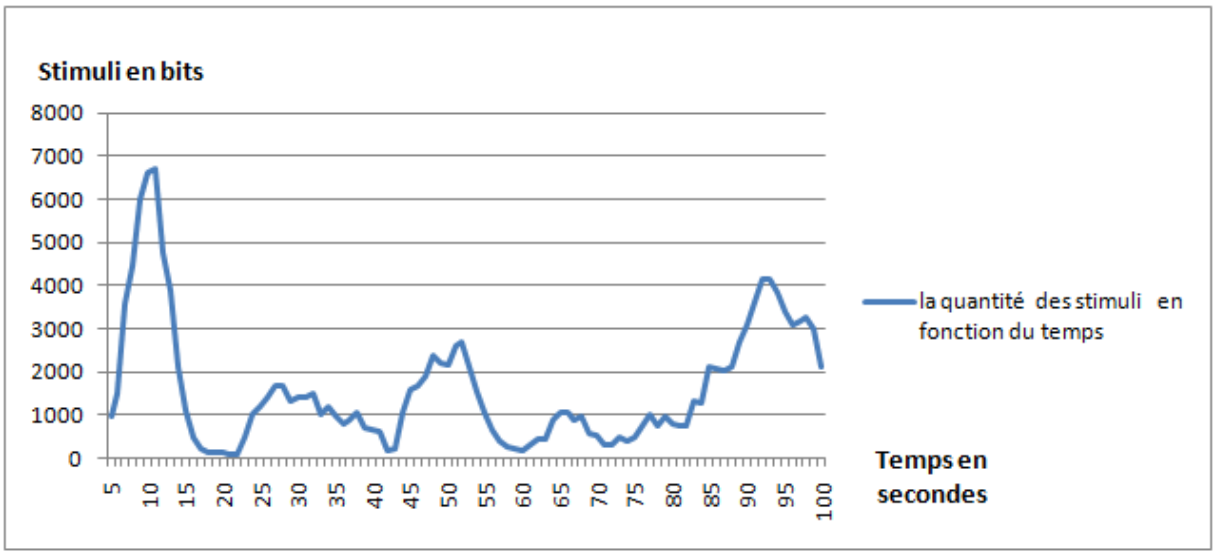

Figure 6.2 La quantité des stimuli des "Targets" reçus par la vraie station de base en fonction du temps

6.3.2 Les paquets AODV au niveau de la station de base dans le réseau simulé

La figure 6.3 a pour coordonnées (en x-abscisse) le temps de simulation, et (en y-ordonnée) la quantité en bits de paquets AODV reçus par la station de base. Ces paquets AODV permettent de définir le routage de chemins dans le réseau WSN.

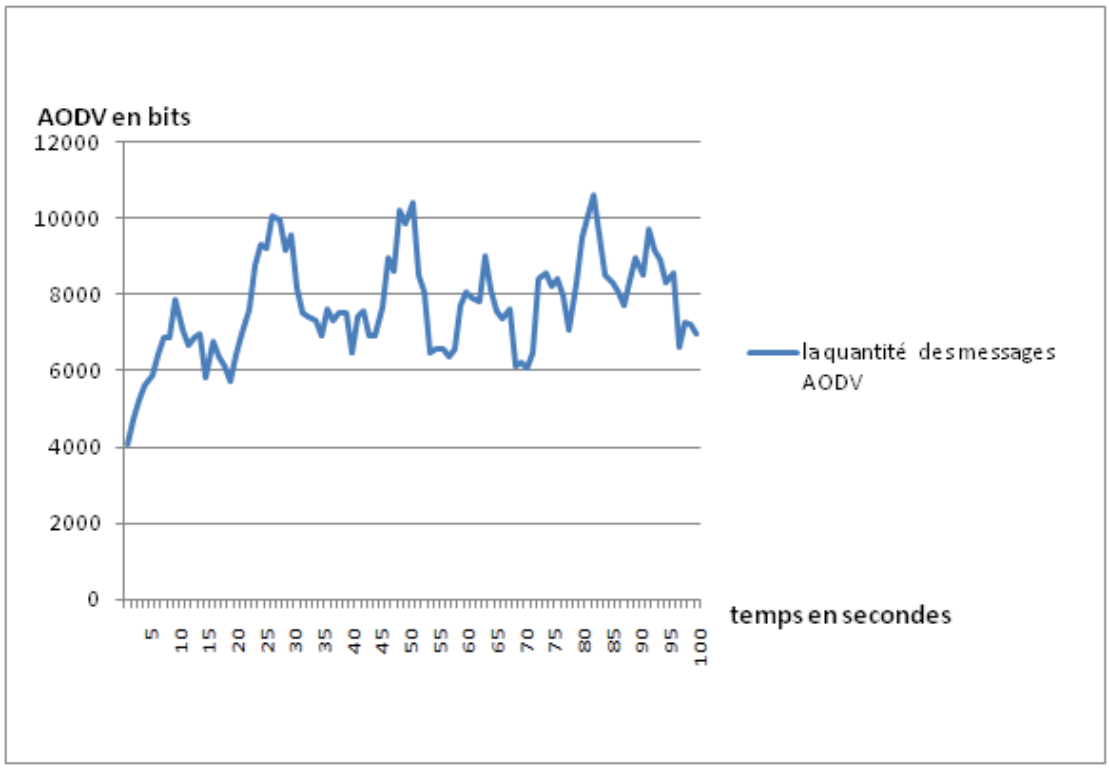

Figure 6.3 La quantité des messages AODV reçus par la vraie station de base en fonction du temps de la simulation.

6.3.3 Les paquets TCP au niveau de la station de base dans le réseau simulé

La figure 6.4 a pour coordonnées (en x-abscisse) le temps de simulation, et (en y-ordonnée) la quantité en bits des paquets TCP reçus par la station de base. Cette figure représente la quantité en bits des messages TCP envoyés par les capteurs du réseau, et reçus par la station de base. Nous constatons que l'envoi des paquets TCP fonctionne correctement dans le réseau. Il est utile de noter que chaque paquet contient 512 octets, alors que chaque stimulus contient 32 octets.

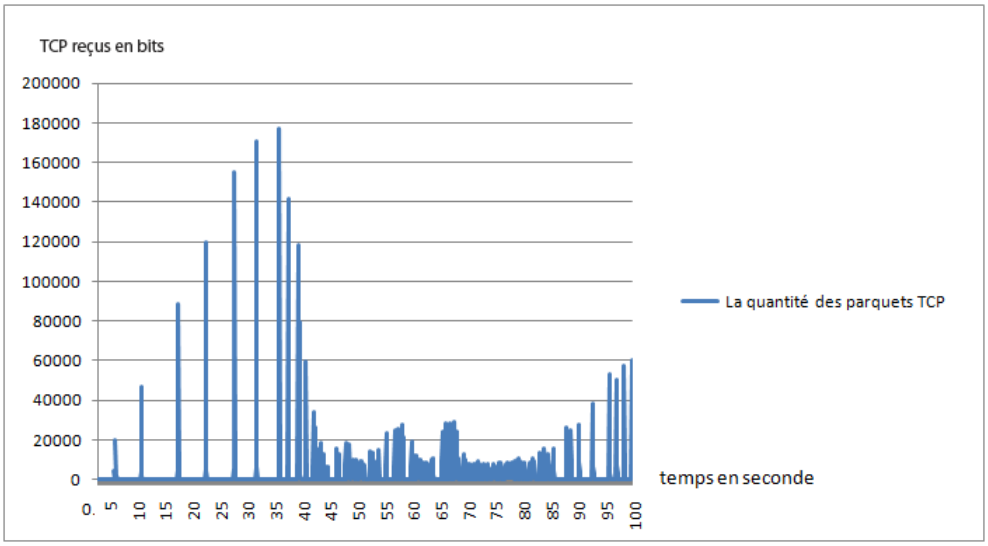

Figure 6.4 La quantité des paquets TCP reçus par la vraie station de base en fonction du temps de simulation.

6.3.4 Les paquets AODV au niveau des capteurs du réseau simulé

La figure 6.5 a pour coordonnées (en x-abscisse) les positions X des capteurs, (en y-ordonnée) les positions Y des capteurs du réseau simulé, et (en z-abscisse) la taille en bits des paquets AODV. Cette figure représente la quantité en bits de la somme des messages AODV reçus par les capteurs à l'instant $t = 100s$ correspondant à la fin de la simulation. Elle montre aussi, que les messages AODV de routage circulent correctement dans le réseau de capteurs sans fil WSN, et montre aussi que le nombre de bits reçus par la région de la station de base est plus élevé que les autres régions du réseau de capteurs sans fil WSN.

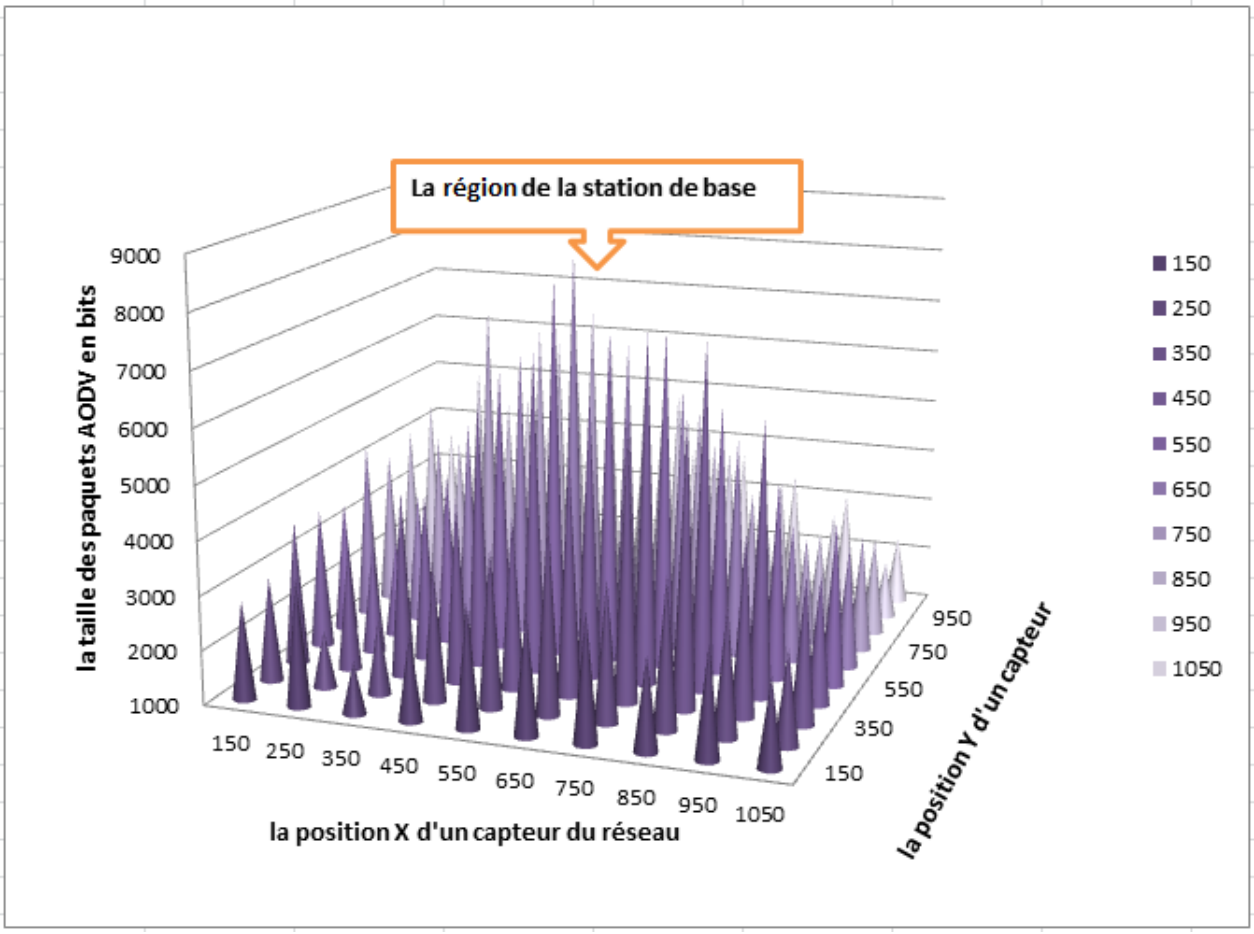

Figure 6.5 La quantité en bits des messages AODV reçus par les capteurs à $t = 100s$.

6.3.5 Les paquets TCP au niveau des capteurs du réseau simulé

La figure 6.6 présente la taille des messages TCP en transmission dans le réseau simulé à l'instant $t = 100s$. Cette figure reprend les principes décrits dans la section 6.3.4, mais en utilisant les paquets TCP au lieu des paquets AODV. Elle montre bien que les messages TCP parviennent à leur destination c.à.d. à la station de base et met en évidence le patron (pattern) d'envoi des messages TCP dans le réseau simulé des capteurs sans fil WSN. Il est utile de noter que nous avons utilisé des paquets TCP ayant 512 octets chacun, au lieu des stimuli de taille individuelle de 32 octets. Ce choix permet d'avoir un trafic beaucoup plus volumineux en TCP qu'en stimuli.

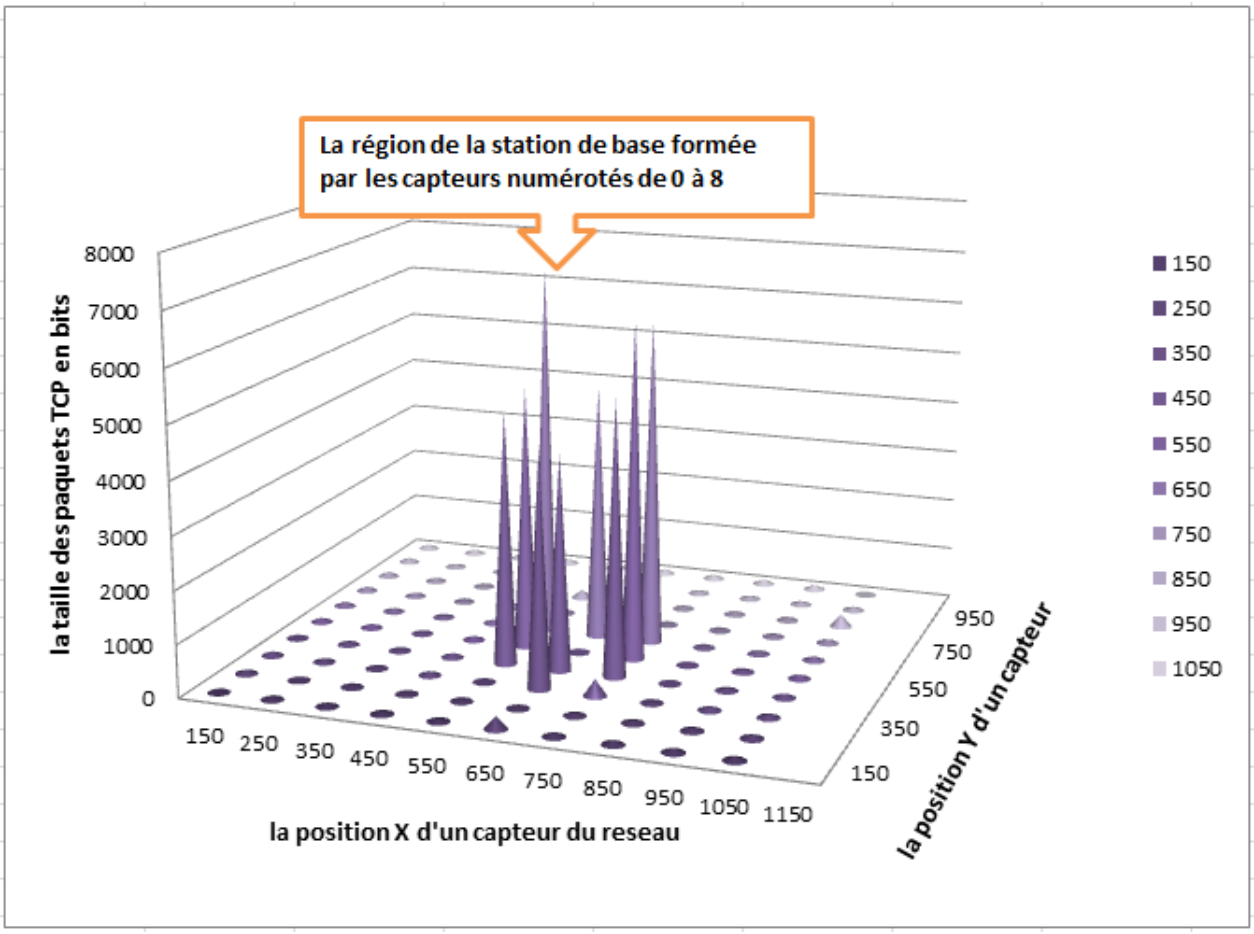

Figure 6.6 La quantité en bits des messages TCP reçus par les capteurs à $t = 100s$

6.4 Interprétation des trafics du réseau simulé

La simulation initiale du réseau de capteurs WSN montre que la station de base et sa région, reçoivent plus de communication que les capteurs intermédiaires éloignés de la station de base. Ceci peut s'expliquer par le fait que tous les capteurs du réseau envoient des messages à la station de base, et que ces messages passent obligatoirement par la région de la station de base. Certains capteurs intermédiaires, ayant un trafic léger, peuvent être utiles pour d'autres fins comme l'envoi d'autres messages à des destinations autres que la station de base.

Une attaque d'analyse de trafic visualise la quantité de paquets en transition sur le réseau, et peut déduire la région de la station de base. Ainsi (en se référant aux figures 6.5 et 6.6), la station de base numérotée 0 et ses capteurs intermédiaires voisins (numérotés de 1 à 8) ont plus de trafic que les autres capteurs numérotés de 9 à 100.

En effet, les figures 6.5 et 6.6 donnent un aperçu de l'allure du trafic au niveau de chaque capteur. L'attaquant analyse les courbes des capteurs de son voisinage, et localise la station de base et ses capteurs voisins. Ainsi, l'attaquant peut s'approcher des capteurs ayant un trafic dense, afin de détecter la position de la station de base, et éventuellement la détruire.

Pour protéger la vraie station de base contre l'attaque d'analyse de trafic, le patron du trafic doit être modifié, afin de cacher le positionnement de la station de base. Comme la région de la station de base connait déjà un trafic important, toute technique de protection doit utiliser au minimum un trafic strictement plus élevé que celui de la station de base et de ses capteurs intermédiaires voisins. Certains capteurs ont un trafic léger, et sont au moins à 3 sauts de la station de base. Il est donc utile d'utiliser un paramètre h pour déterminer le nombre de saut minimum pour le choix des capteurs collaborateurs de la technique de la protection de l'attaque d'analyse de trafic. Le paramètre h permet de diversifier le trafic et de l'étendre dans le réseau WSN.

Notre approche de protection de la station de base, propose donc de créer un nouveau faux trafic dans le réseau de capteurs WSN, en prenant en compte le paramètre s corrrespondant au nombre de capteurs intermédiaires collaborateurs, ayant un trafic léger, et se positionnant au moins à h sauts de la vraie station de base (h est un paramètre du réseau de capteurs sans fil WSN). Ce nouveau trafic a comme destination une fausse station de base, choisie aléatoirement parmi les capteurs intermédiaires à h sauts de la vraie station de base. Elle reçoit du faux trafic TCP, à partir des s capteurs intermédiaires. La fausse station de base, ainsi que les s capteurs intermédiaires sont choisis aléatoirement. La fausse station de base est mobile, et se déplace aléatoirement dans le réseau WSN, avec une périodicité choisie de $T = 33s$. Cette fausse station de base pourrait aussi bien se déplacer autour de la vraie station de base, avec un rayon de h sauts et avec une périodicité choisie de $T = 33s$.

La fausse station de base se déplace périodiquement dans le réseau de capteurs sans fil, et à chaque déplacement, elle crée une région de trafic volumineux autour d'elle, plus élevé que le trafic autour de la vraie station de base, car chaque paquet du faux trafic généré à la source est réputé strictement plus élevé que chaque paquet du vrai trafic. Ainsi, l'attaquant ne peut distinguer une région volumineuse en faux trafic, d'une région volumineuse en vrai trafic. Ceci rend la tâche de localisation de la vraie station de base, par l'attaquant, très difficile. La quantité du vrai trafic de la station de base est supposée connue d'avance.

A notre connaissance, aucune défense n'existe encore contre l'attaque d'analyse de trafic, utilisant une fausse station de base ***mobile***, et recevant des faux paquets. Cependant, Deng

et al. [5] ont utilisé une technique de génération de faux paquets, envoyés aux capteurs voisins et non à une fausse station de base. Elle permet de créer des régions avec un trafic volumineux plus élevé que le trafic de la région de la station de base.

Cependant, notre nouvelle technique de défense utilise une fausse station de base ***mobile***, cette technique n'a pas été abordée à date dans la littérature. Une comparaison entre la défense avec une fausse station de base *statique* vs une fausse station de base *mobile*, est décrite dans le chapitre 7. Elle démontre l'efficacité de la défense avec une fausse station de base mobile. Avec la mobilité de la fausse station de base, l'attaquant ne pourra pas identifier la vraie station de base.

L'hypothèse de cette étude stipule qu'il est possible de créer des régions avec un faux trafic plus volumineux que celui de la région munie du vrai trafic. Ainsi l'attaquant d'analyse de trafic est induit en erreur, et ne peut pas identifier la vraie station de base, et considère que la fausse station de base est la station de base recherchée.

Il est utile de noter, que dans notre étude, nous avons utilisé trois types de données : les paquets AODV, les paquets TCP, et les stimuli. Les paquets AODV sont imposés par le protocole de routage des données dans notre réseau. Nous avons choisi les paquets TCP pour mettre en pratique notre approche, d'autres types de paquets auraient pu être utilisés, et cela sans incidence majeure sur nos résultats. Les stimuli des capteurs "Targets" ont été utilisés simplement, pour vérifier que les informations circulent correctement entre les "Targets" et la vraie station de base, en passant par les capteurs intermédiaires.

6.5 Conclusion

Au cours de ce chapitre, nous avons élaboré et décrit une nouvelle technique de défense contre l'attaque d'analyse de trafic, utilisant l'envoi du faux trafic TCP à une fausse station de base mobile.

Dans le chapitre suivant, nous simulons cette technique pour confirmer que la solution proposée permet bien de cacher la région de la vraie station de base.

CHAPITRE 7

ÉVALUATION ET ANALYSE DES RÉSULTATS DE LA DÉFENSE

Cette analyse vise à évaluer la validité de notre technique, mise en place pour la protection de la station de base. Notre étude implémente la technique de défense contre l'attaque d'analyse de trafic, en utilisant le réseau de capteurs WSN décrit dans le chapitre 6, à l'aide de l'outil J-Sim [6].

Lors de cette étude, un modèle de protection est implémenté, en choisissant d'introduire une fausse station de base mobile, et des capteurs collaborateurs qui envoient des fausses données à cette fausse station de base. La fausse station de base se déplace aléatoirement avec une périodicité prédéfinie de 33 secondes, c.à.d. à l'instant $t = 33s$, $t = 66s$, et $t = 99s$. Pour chaque déplacement, les coordonnées X et Y de la fausse station de base sont choisies aléatoirement entre 0 et 1500 unités. Ces coordonnées pourraient être choisies parmi les positions des capteurs qui se trouvent dans un rayon de h sauts de la vraie station de base.

Avec cette technique, un nouveau faux trafic est créé dans le réseau de capteurs WSN, et ce faux trafic est plus élevé que le vrai trafic, car un faux paquet TCP est de 1024 octets c.à.d. deux fois plus grand qu'un vrai paquet TCP (512 octets). La création de ce nouveau faux trafic perturbe la recherche de la vraie station de base par l'attaquant d'analyse de trafic.

L'attaquant d'analyse de trafic cherche la région ayant le volume de trafic le plus élevé dans le réseau, et en déduit que cette région est la région de la vraie station de base. Cependant, grâce à notre technique, l'attaquant se déplace auprès des régions de la fausse station de base, et s'éloigne de la région de la vraie station de base.

Dans le réseau de capteurs WSN décrit dans le chapitre 7, une valeur h est choisie comme le nombre de sauts d'éloignement de la vraie station de base, et une valeur s est choisie comme le nombre de capteurs collaborateurs. Ensuite, une fausse station de base est choisie aléatoirement parmi les capteurs du réseau, qui sont à h sauts de la vraie station de base. De même, s capteurs collaborateurs sont choisis aléatoirement parmi les capteurs du réseau WSN, à h sauts de la vraie station de base.

Notre technique pourrait traiter plusieurs cas en étudiant plusieurs valeurs de s et h. Parmi les cas possibles :

- Les cas où h est grand et s est grand.
- Les cas où h est grand et s est moyen.
- Les cas où h est grand et s est petit.
- Les cas où h est moyen et s est grand.
- Les cas où h est moyen et s est moyen.
- Les cas où h est moyen et s est petit.
- Les cas où h est petit et s est grand.
- Les cas où h est petit et s est moyen.
- Les cas où h est petit et s est petit.

Dans notre étude, plusieurs cas sont étudiés, en donnant plusieurs valeurs aux paramètres h et s (voir tableau 7.1) :

- Le premier cas est constitué à partir des paramètres $s = 8$ et $h = 3$,
- Le deuxième cas est constitué à partir des paramètres $s = 8$ et $h = 4$,
- Le troisième cas est constitué à partir des paramètres $s = 12$ et $h = 3$.

Tableau 7.1 Les données des trois cas étudiés dans notre mémoire

Paramètres		Liste des capteurs à h hops de la station de base	Numéro de la fausse station de base	Numéros des capteurs collaborateurs
s	h			
8	3	26 à 100	47	27, 46, 48, 76, 77, 78, 79, 80
8	4	50 à 100	58	51, 53, 63, 73, 74, 98, 99, 100
12	3	26 à 100	68	28, 31, 35, 53, 63, 84, 88, 89, 91, 93, 97, 100

L'analyse de ces trois cas permet d'évaluer l'influence des paramètres h et s sur l'efficacité de la technique de la protection contre l'attaque d'analyse de trafic. En effet, la différence entre le premier cas et le deuxième cas réside dans la modification du paramètre h, alors que la différence entre le premier cas et le troisième cas est la modification de la valeur s. Notre objectif est de faire varier les valeurs de s et de h, afin de vérifier si la solution proposée dépend de ces deux variables. Pour cela, nous analysons l'effet de la modification des deux paramètres h et s sur l'allure du faux trafic dans le réseau WSN.

Les figures 7.1 à 7.17 décrivent les trafics dans notre réseau de capteurs WSN simulé. Les coordonnées X, Y , et Z de ces figures sont détaillées dans le tableau 7.2).

Tableau 7.2 La description des axes des figures des trafics dans le réseau simulé.

Les figures	L'axe X	L'axe Y	L'axe Z
La figure 7.1, 7.2, et 7.3	Le temps de simulation.	La quantité en bits des paquets reçus par la vraie station de base, et par la fausse station de base.	Sans objet.
La figure 7.4, 7.5, et 7.6	Le temps de simulation.	La quantité en bits de stimuli reçus par la vraie station de base, et celle reçue par la fausse station de base.	Sans objet.
La figure 7.7, 7.8, et 7.9	Le temps de simulation.	La quantité des paquets AODV reçus par chacune des deux stations de base.	Sans objet.
La figure 7.10, 7.11, 7.12, et 7.13	Les positions X des capteurs du réseau simulé.	Les positions Y des capteurs du réseau simulé.	La taille en bits des paquets TCP reçus par chaque capteur à l'instant $t = 100$ secondes.
La figure 7.14, 7.15, 7.16, et 7.17	Les positions X des capteurs du réseau simulé.	Les positions Y des capteurs du réseau simulé.	La taille des paquets AODV en bits reçus par chaque capteur à l'instant $t = 100$ secondes.

7.1 Les hypothèses des cas simulés

Le trafic est généré dans tout le réseau en utilisant le simulateur J-Sim, pour une simulation de 100 secondes, avec un pas de rafraichissement de 1 seconde.

Ci-dessous, la description des hypothèses des trois cas simulés.

7.1.1 Cas 1 ($h = 3$, $s = 8$)

Une fausse station de base est introduite pour protéger le réseau simulé de l'attaque d'analyse de trafic. La liste des capteurs qui sont au moins de $h = 3$ sauts de la vraie station de base est constituée des capteurs numérotés de 26 à 100. La fausse station de base numérotée

47 est choisie parmi les capteurs 26 à 100. Ensuite, $s = 8$ capteurs collaborateurs sont choisis aléatoirement parmi cette même liste des capteurs numérotés de 26 à 100 (en générant un nombre aléatoire dans l'intervalle [26..100]). Ces capteurs collaborateurs sont définis dans la liste suivante $\{27, 46, 48, 76, 77, 78, 79, 80\}$. Ils ont un module "TCP source" qui permet de générer de faux paquets TCP de taille 1024 bits à destination de la fausse station de base. Cette fausse station de base dispose d'un module "TCP Sink" qui permet de recevoir les faux messages TCP envoyés par les capteurs collaborateurs.

Les figures 7.1, 7.4, 7.7, 7.10, et 7.14 montrent l'impact de l'introduction du faux trafic, sur un réseau de capteurs WSN.

En effet, les courbes 7.10 et 7.14, en présence d'une fausse station de base, donnent un aperçu du patron (pattern) du trafic à chaque niveau de capteur. L'attaquant analyse ce trafic, et il déduit la position de la station de base et de ses capteurs voisins. Ainsi, l'attaquant peut s'approcher de plus en plus des capteurs ayant un trafic volumineux (ce trafic pouvant être un vrai ou un faux trafic), afin de détecter la position de la station de base et éventuellement la détruire.

7.1.2 Cas 2 ($h = 4$, $s = 8$)

Pour vérifier l'influence des paramètres h et s, nous étudions différents cas, avec des valeurs différentes de h et s. Les mêmes éléments que le cas 1 sont repris dans le cas 2 à quelques différences près, à savoir :

- La liste des capteurs qui sont au moins de $h = 4$ sauts de la vraie station de base est constituée à partir des capteurs numérotés de 50 à 100.
- La fausse station de base numérotée 58 est alors choisie parmi les capteurs de 50 à 100
- $s = 8$ capteurs collaborateurs choisis aléatoirement, et définis dans la liste suivante : $\{51, 53, 63, 73, 74, 98, 99, 100\}$

Les figures 7.2, 7.5, 7.8, 7.11, et 7.15 montrent le patron (pattern) des trafics autour de la vraie station de base et la fausse station de base, et aussi autour des capteurs du réseau WSN.

7.1.3 Cas 3 ($h = 3$, $s = 12$)

Les mêmes éléments que le cas 1 sont repris dans le cas 3 à quelques différences près, à savoir :

- Une fausse station de base numérotée 68, est alors choisie parmi les capteurs numéroté de 26 à 100 (voir le tableau 7.1).
- $s = 12$ capteurs collaborateurs choisis aléatoirement et définis dans la liste suivante {28, 31, 35, 53, 63, 84, 88, 89, 91, 93,97, 100}
- Les figures 7.3, 7.6, 7.9, 7.12, et 7.16 montrent le patron (pattern) du trafic autour de la vraie station de base, la fausse station de base, et autour des capteurs du réseau WSN.

7.2 Le trafic TCP au niveau des stations de base

Le tableau 7.2 indique les coordonnées utilisées dans les figures 7.1, 7.2 et 7.3. Le tableau 7.3 en interprète les résultats. Ces figures représentent la quantité en bits des paquets TCP reçus par la vraie station de base numérotée 0, et par la fausse station de base numérotée successivement 47, 58 et 68 selon les cas 1, 2 et 3 (voir le tableau 7.1). Elles montrent bien que l'ensemble du vrai trafic TCP parvient à sa destination c.à.d. la vraie station de base, alors que le faux trafic TCP transite vers la fausse station de base. Ces figures montrent aussi que le faux trafic TCP est plus élevé que le vrai trafic TCP (car un faux paquet TCP est de 1024 octets c.à.d. deux fois plus grand qu'un vrai paquet TCP), ce qui ne permet pas à l'attaquant de localiser la vraie station de base.

7.2.1 Cas 1 ($h = 3$, $s = 8$)

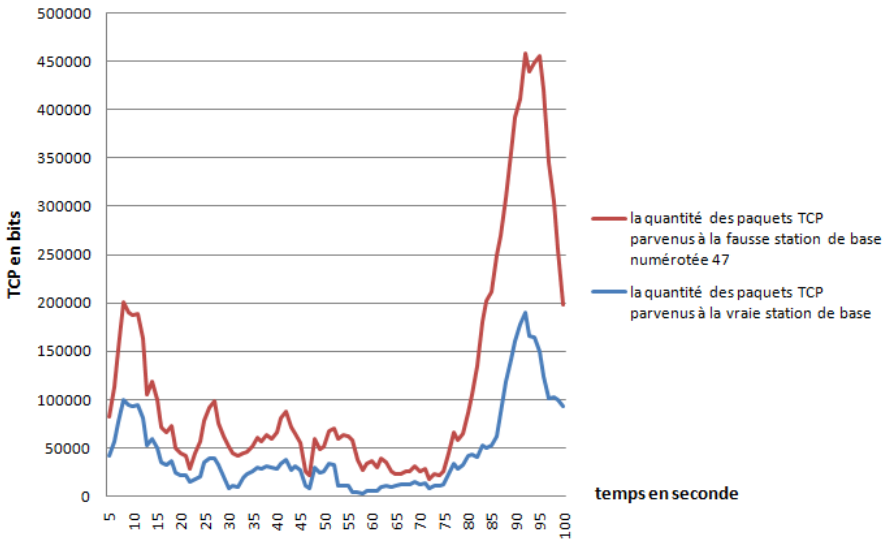

Figure 7.1 La quantité en bits des paquets TCP parvenus à la vraie station de base et à la fausse station de base numérotée par 47 en fonction du temps de la simulation et par pas de 5 secondes.

7.2.2 Cas 2 ($h = 4,\ s = 8$)

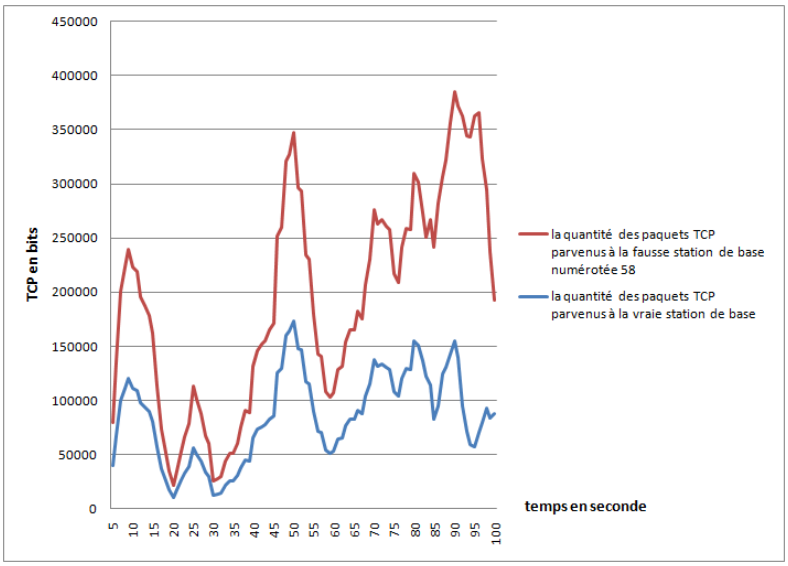

Figure 7.2 La quantité des paquets TCP parvenus à la vraie station de base et à la fausse station de base numérotée 58 en fonction du temps de la simulation et par pas de 5 secondes.

7.2.3 Cas 3 ($h = 3,\ s = 12$)

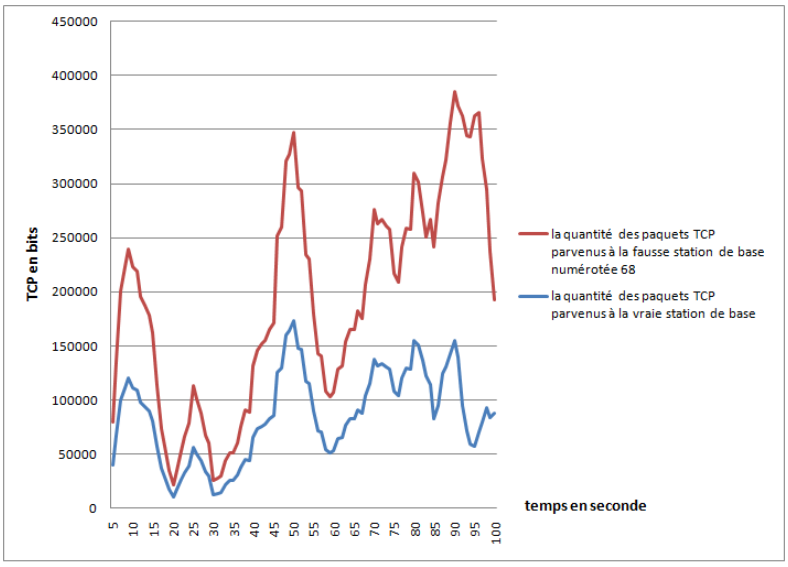

Figure 7.3 La quantité des paquets TCP parvenus à la vraie station de base et à la fausse station de base numérotée 68 en fonction du temps de la simulation et par pas de 5 secondes.

7.3 Le trafic des stimuli au niveau des stations de base

Le tableau 7.2 indique les coordonnées utilisées dans les figures 7.4, 7.5 et 7.6. Le tableau 7.3 en interprète les résultats. Ces figures représentent la quantité de stimuli reçue par la vraie station de base, et celle reçue par la fausse station de base numérotée successivement 47, 58 et 68 selon les cas 1, 2 et 3. Elles montrent bien que la totalité des stimuli arrivent à la vraie station de base, et qu'aucun stimulus ne parvient à la fausse station de base, ainsi toute l'information des stimuli ne se perd pas dans le réseau, et parvient effectivement à la bonne destination.

7.3.1 Cas 1 ($h = 3$, $s = 8$)

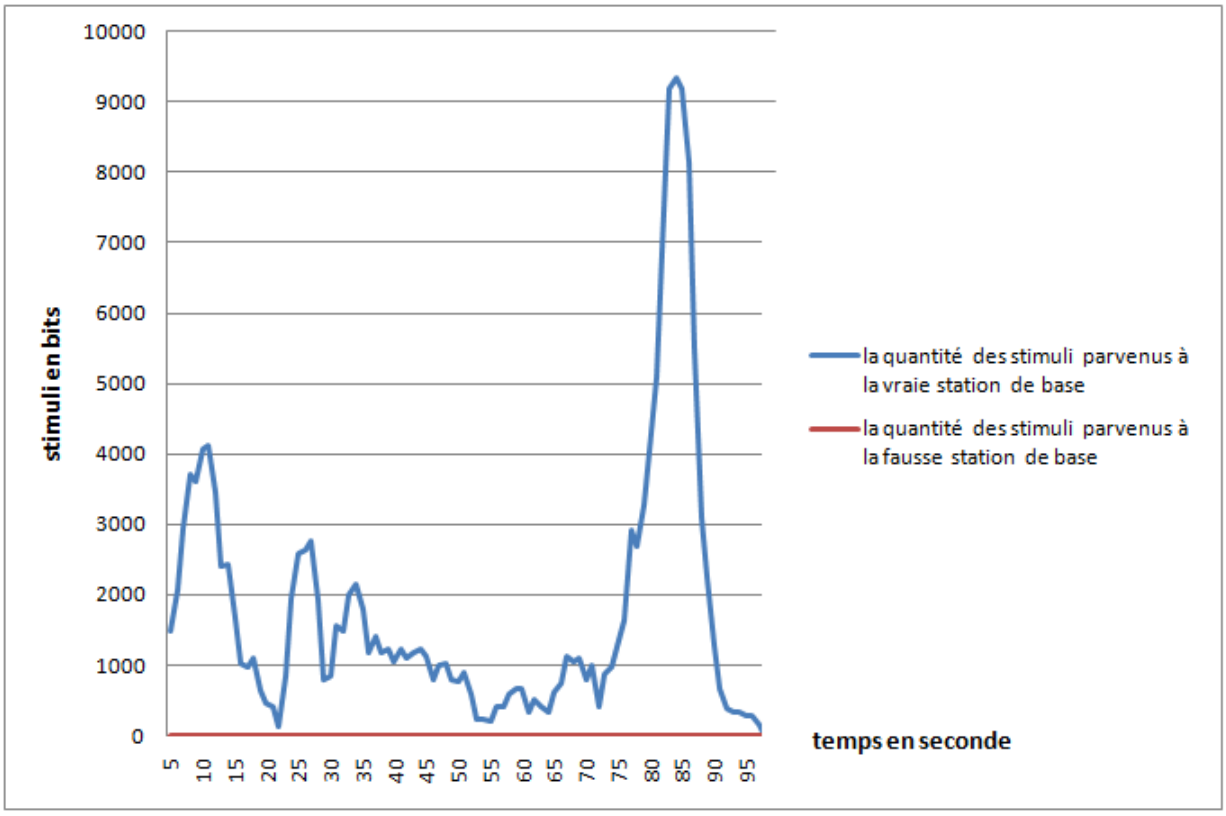

Figure 7.4 La quantité des stimuli parvenus à la vraie station de base et à la fausse station de base numérotée 47 en fonction du temps de la simulation.

7.3.2 Cas 2 ($h = 4,\ s = 8$)

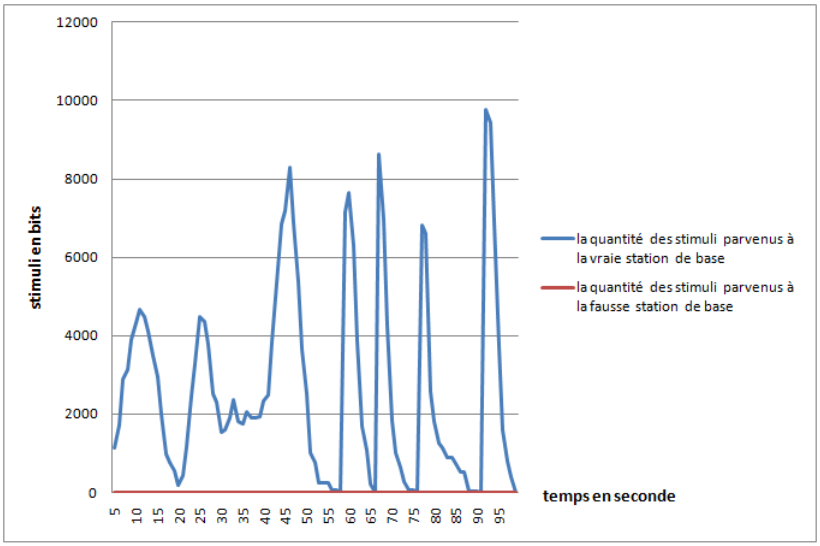

Figure 7.5 La quantité des stimuli parvenus à la vraie station de base et à la fausse station de base numérotée 58 en fonction du temps de la simulation.

7.3.3 Cas 3 ($h = 3,\ s = 12$)

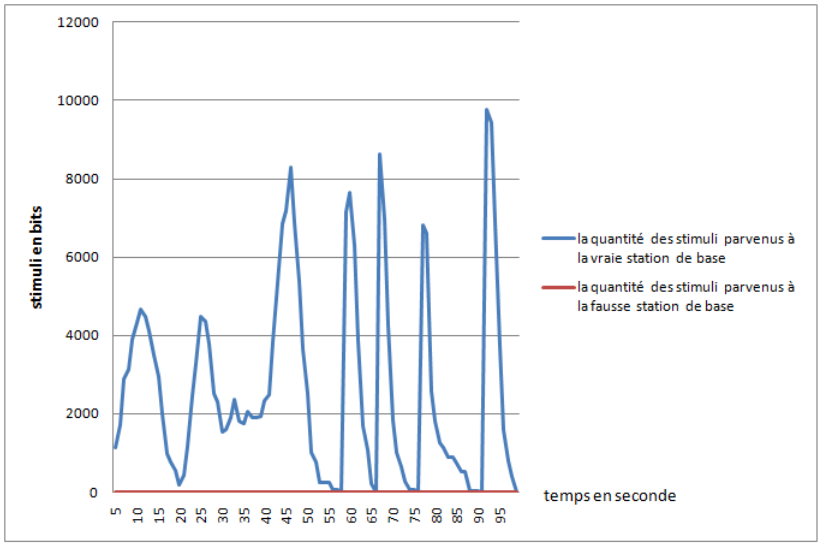

Figure 7.6 La quantité des stimuli parvenus à la vraie station de base et à la fausse station de base numérotée 68 en fonction du temps de la simulation.

7.4 Le trafic AODV au niveau de la vraie et la fausse station de base

Le tableau 7.2 indique les coordonnées utilisées dans les figures 7.7, 7.8, et 7.9. Le tableau 7.3 en interprète les résultats. Ces figures représentent la quantité en bits des paquets AODV reçus par la vraie station de base numérotée 0, et par la fausse station de base numérotée successivement 47, 58 et 68 selon les cas 1, 2 et 3. Elles montrent bien que les paquets AODV de routage fonctionnent correctement dans le réseau WSN simulé, car les stations de base recoivent bien les bons paquets AODV.

7.4.1 Cas 1 ($h = 3$, $s = 8$)

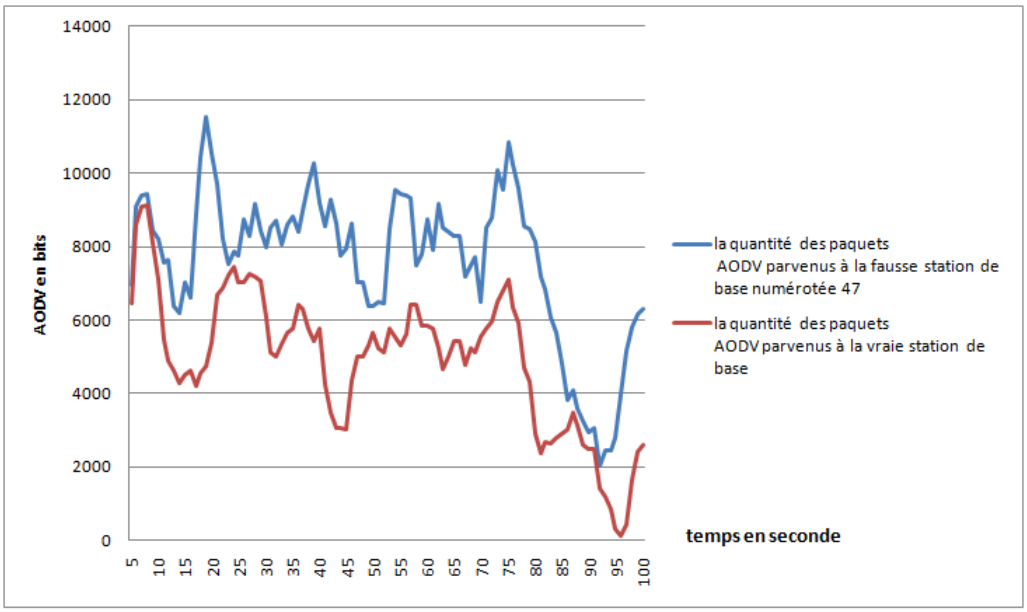

Figure 7.7 La quantité des paquets AODV parvenus à la vraie station de base et à la fausse station de base numérotée 47 en fonction du temps de la simulation.

7.4.2 Cas 2 ($h = 4$, $s = 8$)

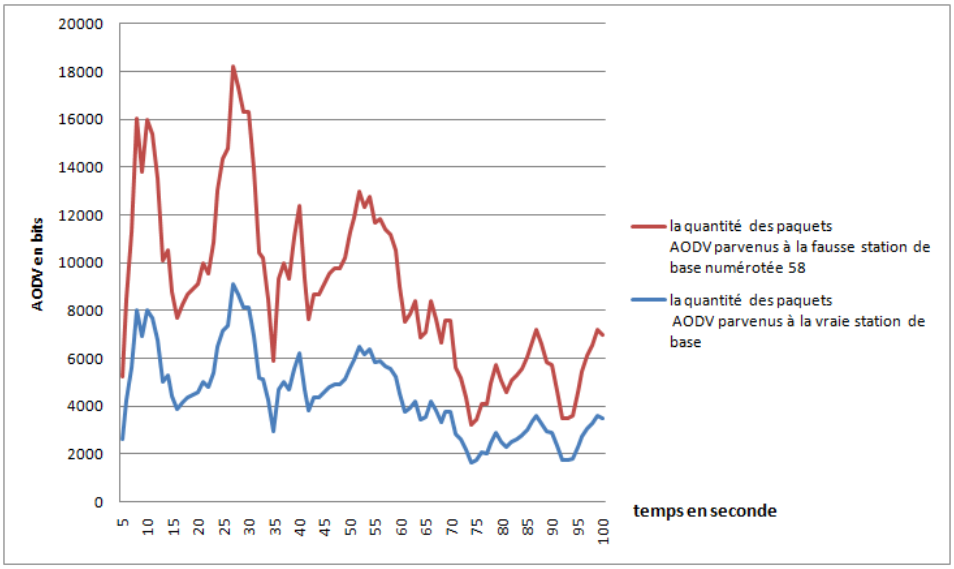

Figure 7.8 La quantité des paquets AODV parvenus à la vraie station de base et à la fausse station de base numérotée 58 en fonction du temps de la simulation.

7.4.3 Cas 3 ($h = 3$, $s = 12$)

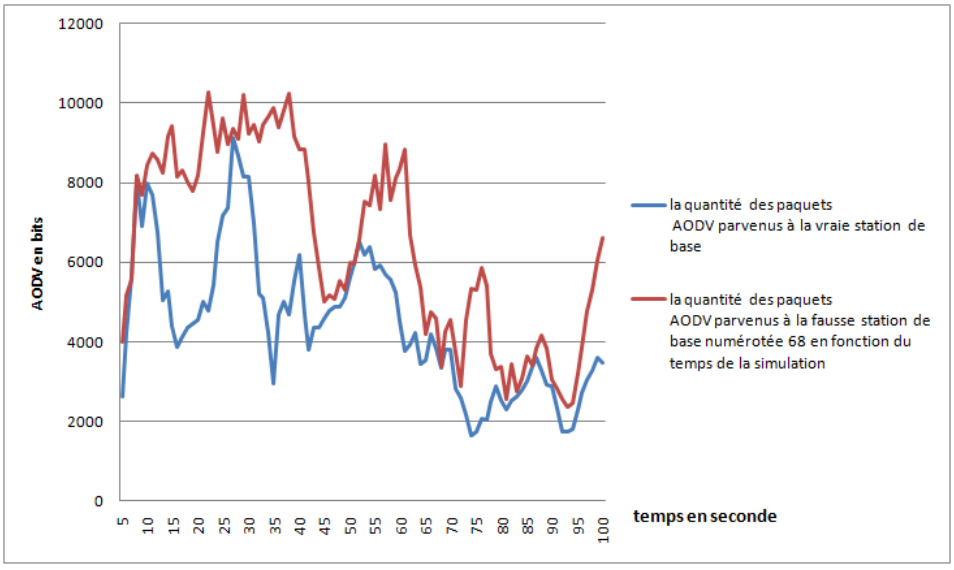

Figure 7.9 La quantité des paquets AODV parvenus à la vraie station de base et à la fausse station de base numérotée 68 en fonction du temps de la simulation.

7.5 Le trafic TCP au niveau des capteurs du réseau simulé WSN

Le tableau 7.2 indique les coordonnées utilisées dans les figures 7.10, 7.11, 7.12 et 7.13. Le tableau 7.3 en interprète les résultats. Ces figures montrent bien le contraste entre le patron (pattern) du trafic TCP dans le réseau de capteurs sans fil WSN simulé, et les régions munies de trafic volumineux surtout dans la région de la fausse station de base.

7.5.1 Cas 1 ($h = 3$, $s = 8$)

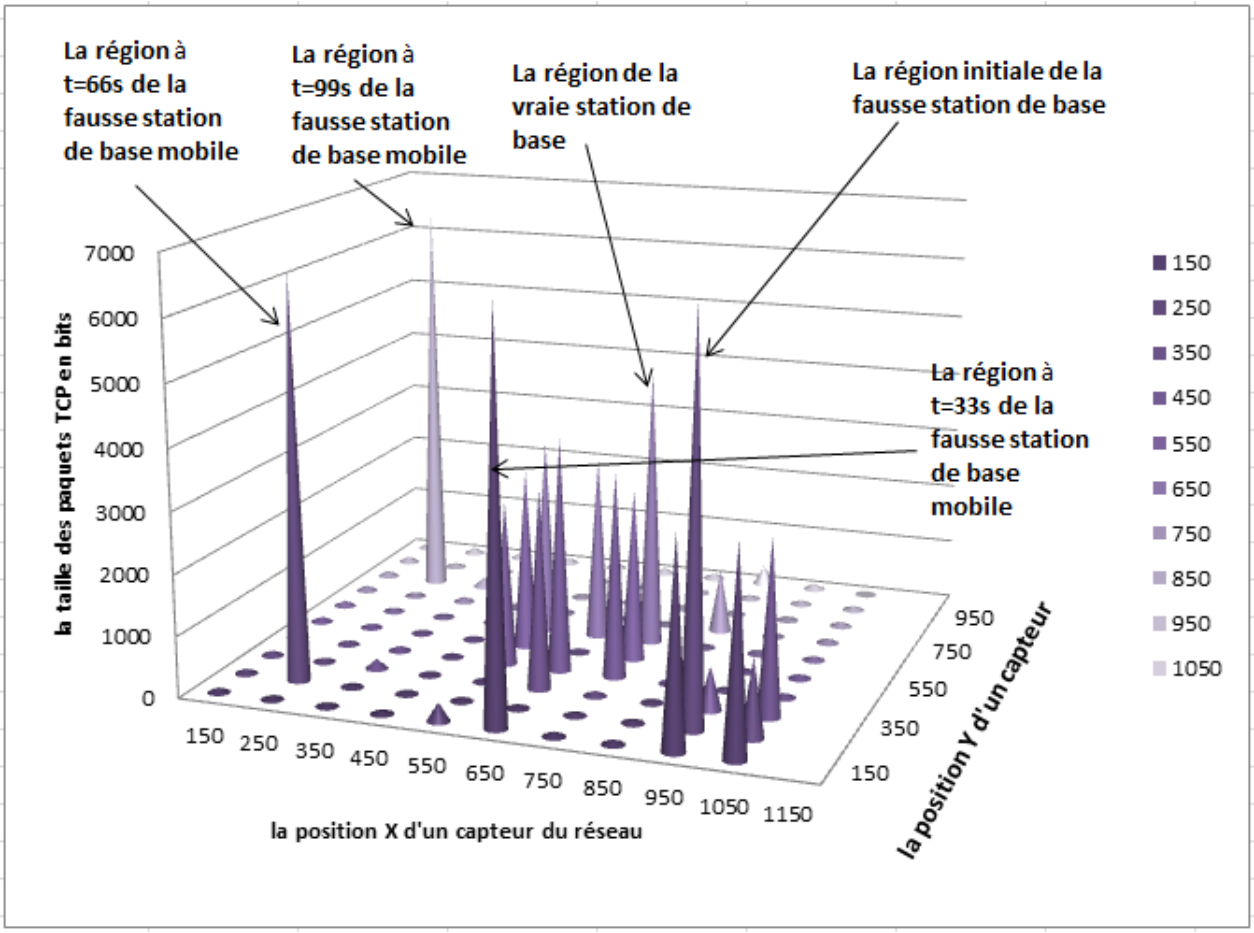

Figure 7.10 Le patron (pattern) de la somme de tous les paquets TCP dans le réseau simulé de capteurs sans fil WSN à l'instant $t = 100s$. Les régions à $t = 0s$, $t = 33s$, et $t = 66s$ représentent l'emplacement de la fausse station de base en fonction du temps.

7.5.2 Cas 2 ($h = 4,\ s = 8$)

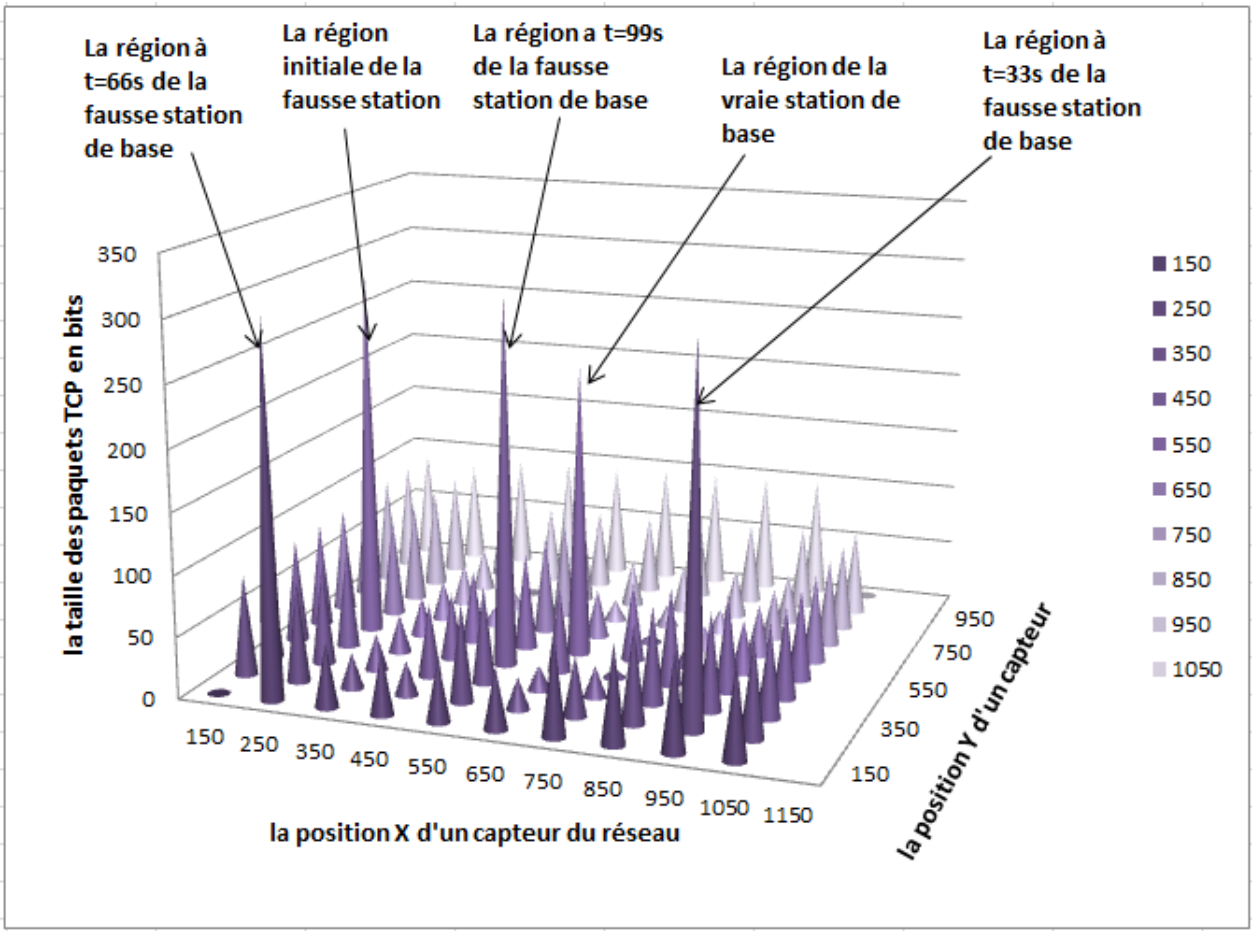

Figure 7.11 Le patron des paquets TCP dans le réseau simulé de capteurs sans fil WSN à l'instant $t = 100s$. Les régions à $t = 0s$, $t = 33s$, et $t = 66s$ représentent l'emplacement de la fausse station de base en fonction du temps.

7.5.3 Cas 3 ($h = 3,\ s = 12$)

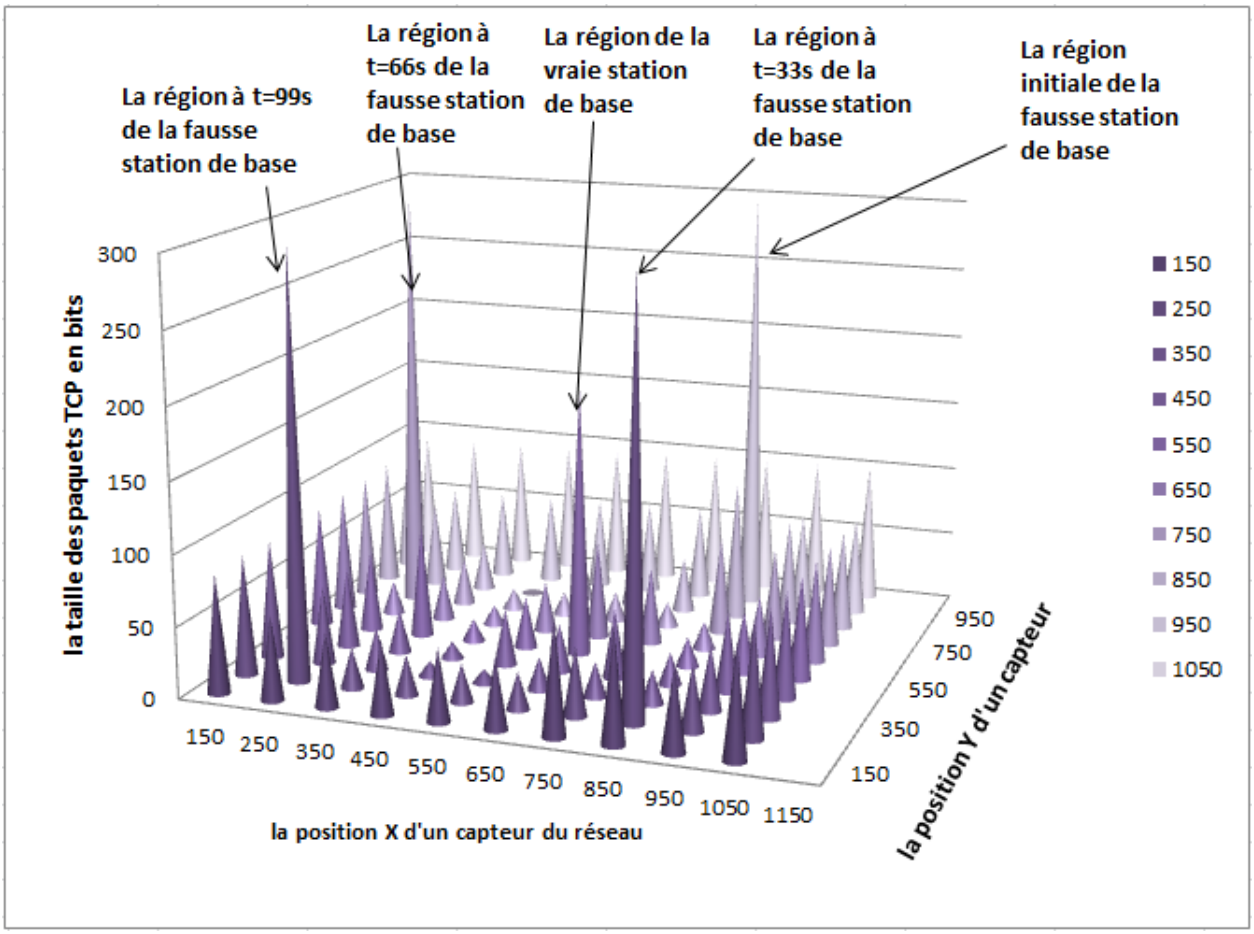

Figure 7.12 Le patron de la somme de tous les paquets TCP dans le réseau simulé de capteurs sans fil WSN à l'instant $t = 100s$. Les régions à $t = 0s$, $t = 33s$, et $t = 66s$ représentent l'emplacement de la fausse station de base en fonction du temps.

7.5.4 Cas 1 muni d'une trajectoire circulaire de la fausse station de base ($h = 3$, $s = 8$)

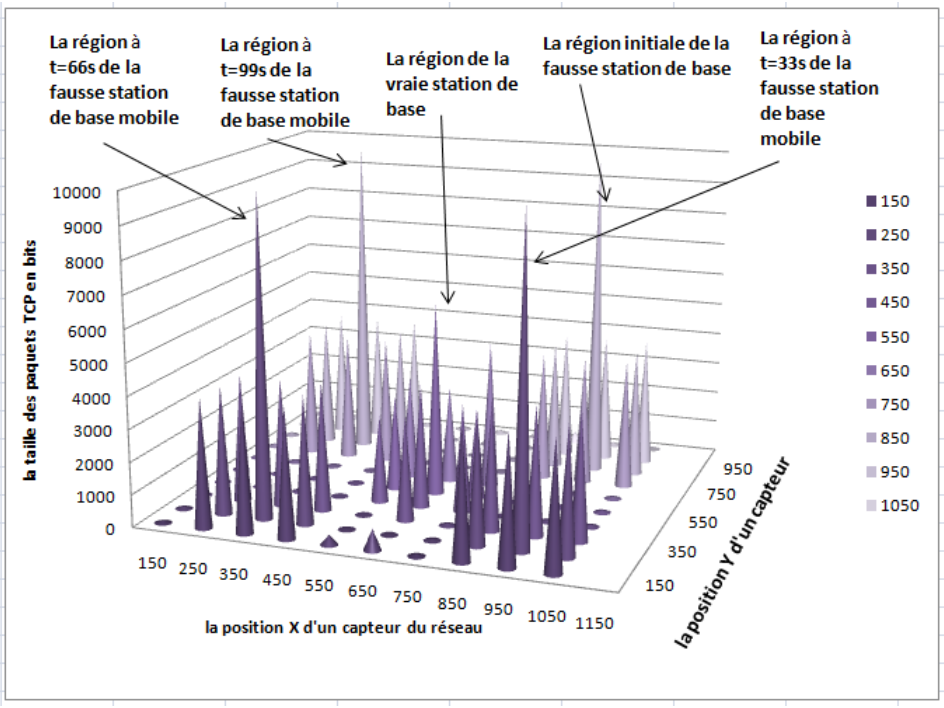

Figure 7.13 Le patron (pattern) de la somme de tous les paquets TCP dans le réseau simulé de capteurs sans fil WSN à l'instant $t = 100s$. Les régions à $t = 0s$, $t = 33s$, et $t = 66s$ représentent l'emplacement de la fausse station de base en fonction du temps. La fausse station de base se deplace sur une trajectoire circulaire de rayon de $h = 3$ sauts.

7.6 Le trafic AODV au niveau des capteurs du réseau simulé WSN

Le tableau 7.2 indique les coordonnées utilisées dans les figures 7.14, 7.15, 7.16, et 7.17. Le tableau 7.3 en interprète les résultats. Ces figures montrent bien le contraste entre le patron (pattern) du trafic AODV dans le réseau de capteurs sans fil WSN simulé, et les régions munies de trafic volumineux surtout dans la région de la fausse station de base.

7.6.1 Cas 1 ($h = 3,\ s = 8$)

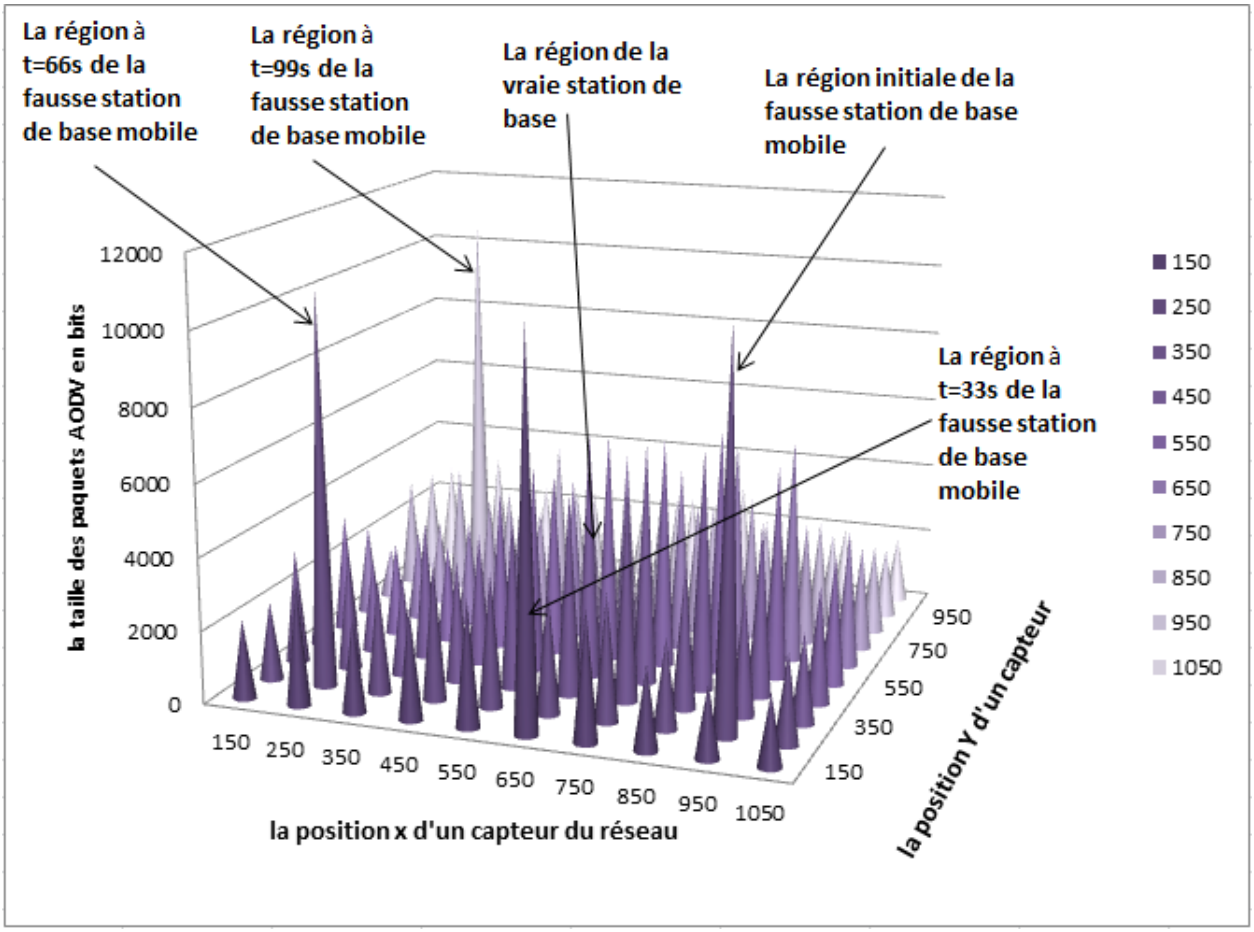

Figure 7.14 Le patron du trafic AODV dans le réseau simulé de capteurs sans fil WSN à l'instant $t = 100s$. Les régions à $t = 0s$, $t = 33s$, et $t = 66s$ représentent l'emplacement de la fausse station de base en fonction du temps.

7.6.2 Cas 2 ($h = 4$, $s = 8$)

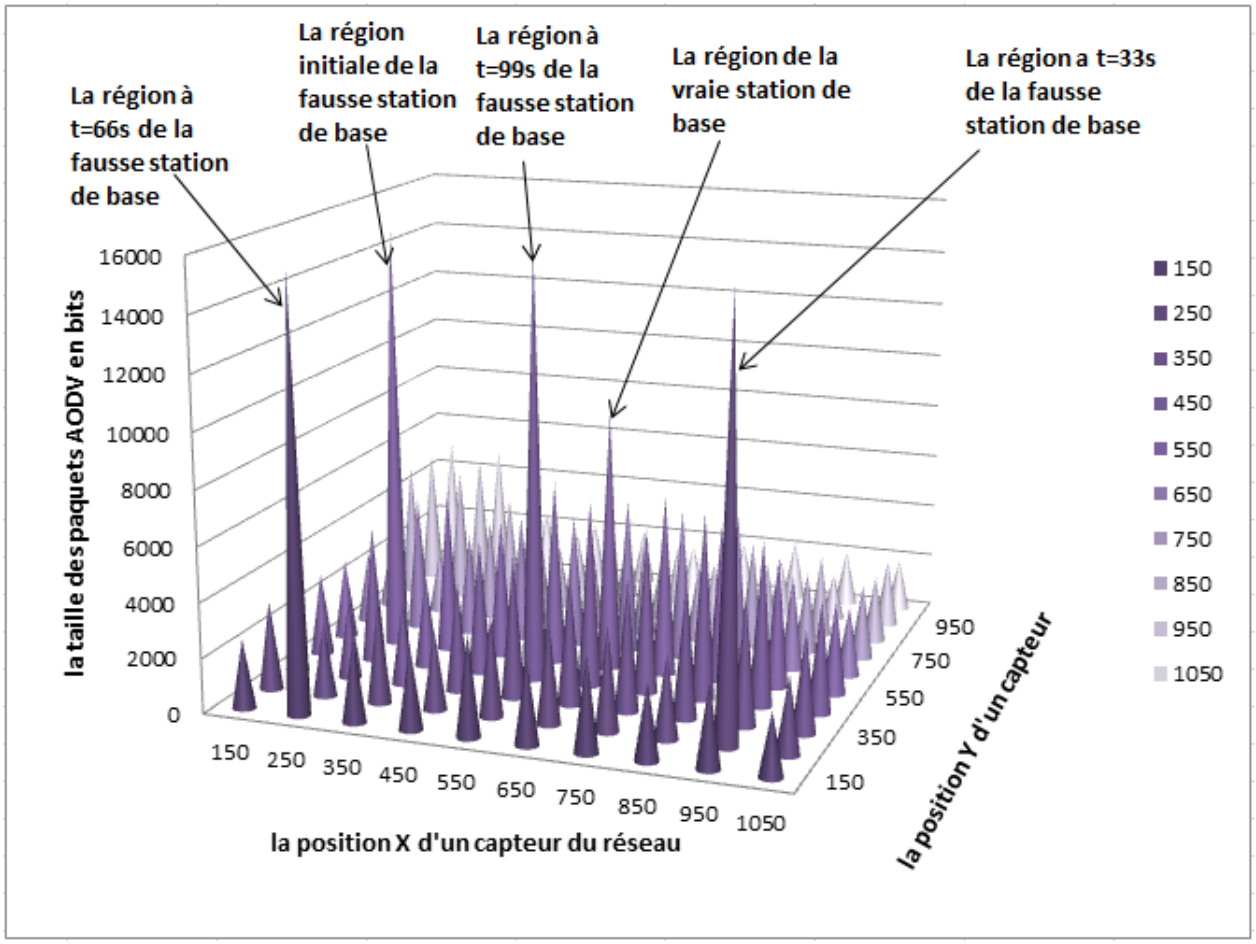

Figure 7.15 Le patron du trafic AODV dans le réseau simulé de capteurs sans fil WSN à l'instant $t = 100s$. Les régions à $t = 0s$, $t = 33s$, et $t = 66s$ représentent l'emplacement de la fausse station de base en fonction du temps.

7.6.3 Cas 3 ($h = 3,\ s = 12$)

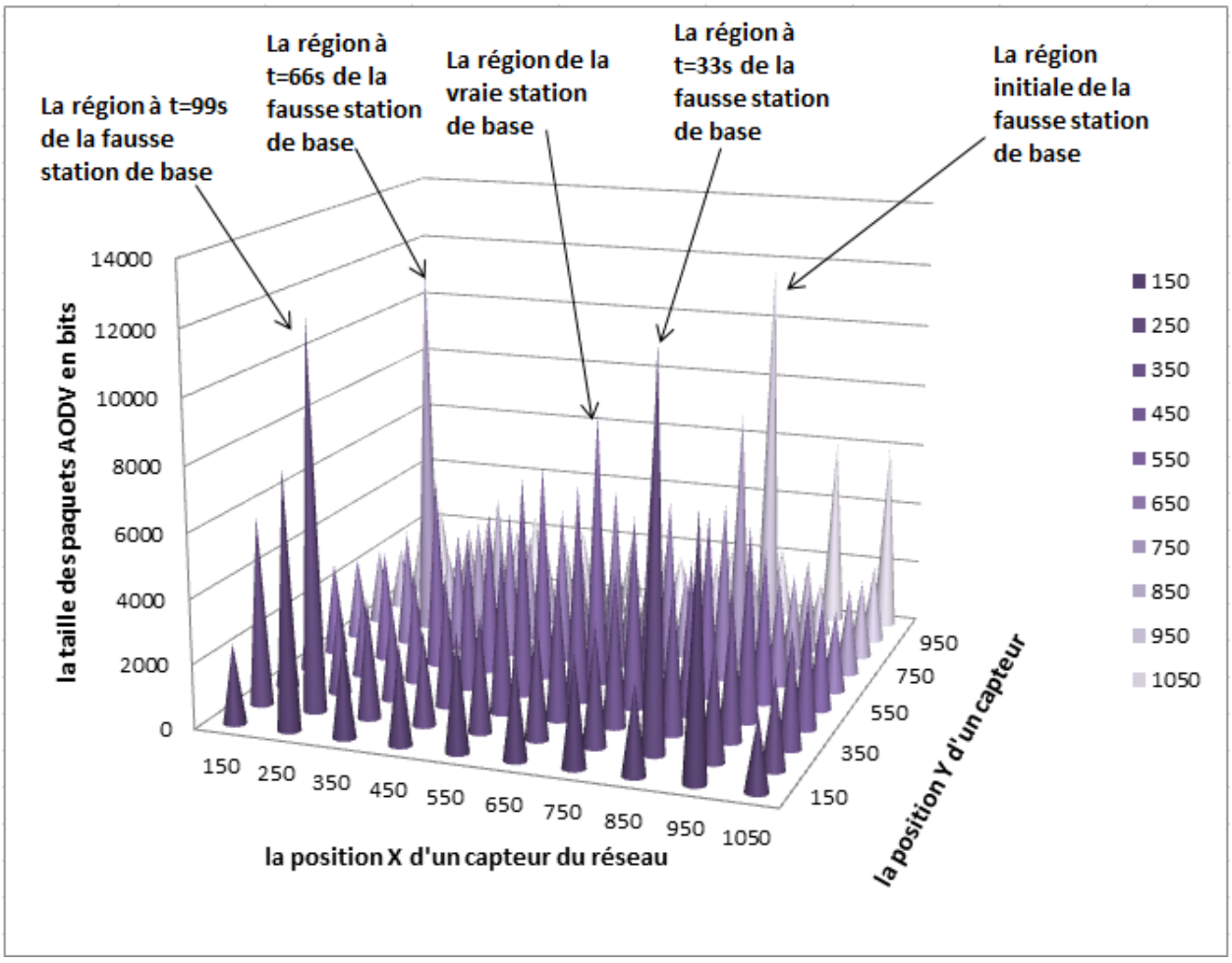

Figure 7.16 Le patron du trafic AODV dans le réseau simulé de capteurs sans fil WSN à l'instant $t = 100s$. Les régions à $t = 0s$, $t = 33s$, et $t = 66s$ représentent l'emplacement de la fausse station de base en fonction du temps.

7.6.4 Cas 1 muni d'une trajectoire circulaire de la fausse station de base ($h = 3$, $s = 8$)

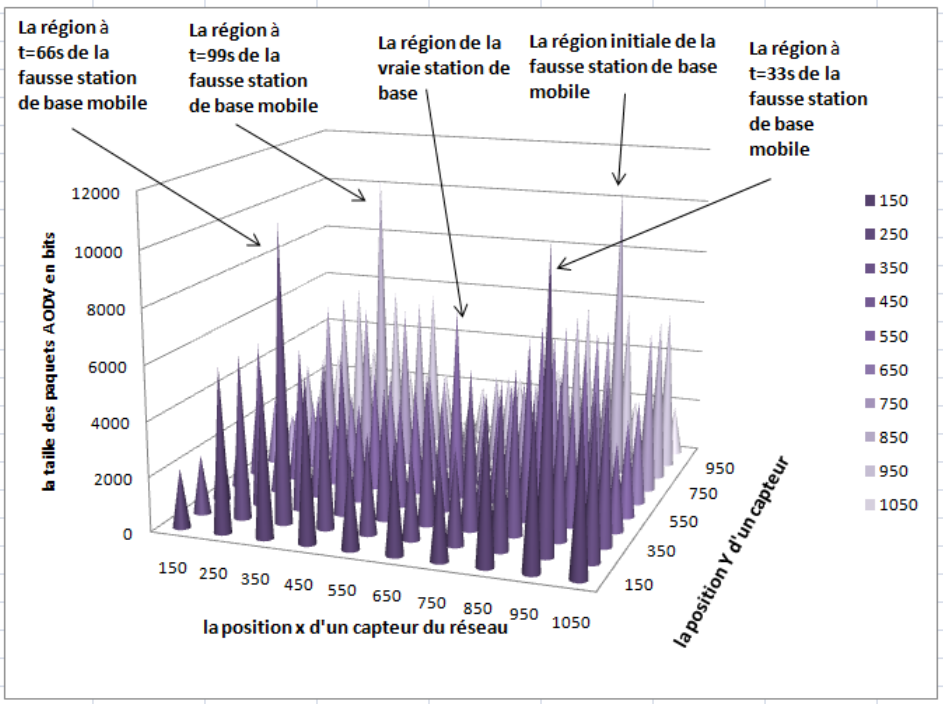

Figure 7.17 Le patron (pattern) de la somme de tous les paquets AODV dans le réseau simulé de capteurs sans fil WSN à l'instant $t = 100s$. Les régions à $t = 0s$, $t = 33s$, et $t = 66s$ représentent l'emplacement de la fausse station de base en fonction du temps. La fausse station de base se déplace sur une trajectoire circulaire de rayon de $h = 3$ sauts.

7.7 Les autres cas possibles

Plusieurs cas, différents des trois cas étudiés auparavant, sont possibles. Les valeurs du paramètre h peuvent varier de 1 au *saut maximum* de la vraie station de base (dans notre simulation : *saut maximum*= 5). Les valeurs du paramètre s peuvent varier de 1 jusqu'au *nombre total des capteurs du réseau* -1. Il est utile de noter que plus la valeur de s est grande, plus le volume du faux trafic créé est grand et plus l'énergie est consommée. De même, plus la valeur de h est grande, plus le faux trafic est dispersé dans le réseau de capteurs WSN.

Nous pouvons regrouper ces différents cas selon les catégories suivantes :

- Catégorie I : où h est grand et s est grand.
- Catégorie II : où h est grand et s est moyen.
- Catégorie III : où h est grand et s est petit.

- Catégorie VI : où h est moyen et s est grand.
- Catégorie V : où h est moyen et s est moyen.
- Catégorie VI : où h est moyen et s est petit.
- Catégorie VII : où h est petit et s est grand.
- Catégorie VIII : où h est petit et s est moyen.
- Catégorie IX : où h est petit et s est petit.

Dans notre simulation, les paramètres h et s peuvent varier dans les intervalles [1..5] et [1..99] respectivement. Nous divisons ces intervalles en trois parties pour déterminer les petites, moyennes et grandes valeurs des deux paramètres h et s. Donc, nous considérons :

- Pour le paramètre h : 4 et 5 sont des grandes valeurs, 3 est une valeur moyenne, et 1 et 2 sont des valeurs petites.
- Pour le paramètre s : 67 à 99 sont des grandes valeurs, 34 à 66 sont des valeurs moyennes, et 1 à 33 sont des valeurs petites.

La simulation, des différents cas de chaque catégorie (voir 7.7) de notre réseau WSN, montre que les résultats des catégories I à IV (voir 7.7) ne sont pas satisfaisants car le faux trafic généré est très dispersé dans le réseau. Les résultats de la simulation des cas de la catégorie VII (voir 7.7) sont satisfaisants sauf que l'énergie du réseau WSN est grandement consommée. Les résultats de la simulation de la catégorie VIII (voir 7.7) sont plus intéressants que ceux de la catégorie IX (voir 7.7) parce que le faux trafic de la catégorie VIII est plus volumineux que celui de la catégorie IX.

7.8 Le déplacement de l'attaquant dans le réseau des capteurs simulé WSN

L'attaquant se déplace dans son entourage, avec une périodicité d'une seconde, vers le capteur ayant plus de trafic que ses voisins. Sa position initiale dans le réseau WSN est aléatoire. Cet attaquant cesse de se déplacer quand le capteur de sa position courante a plus de trafic que tous les capteurs de son entourage.

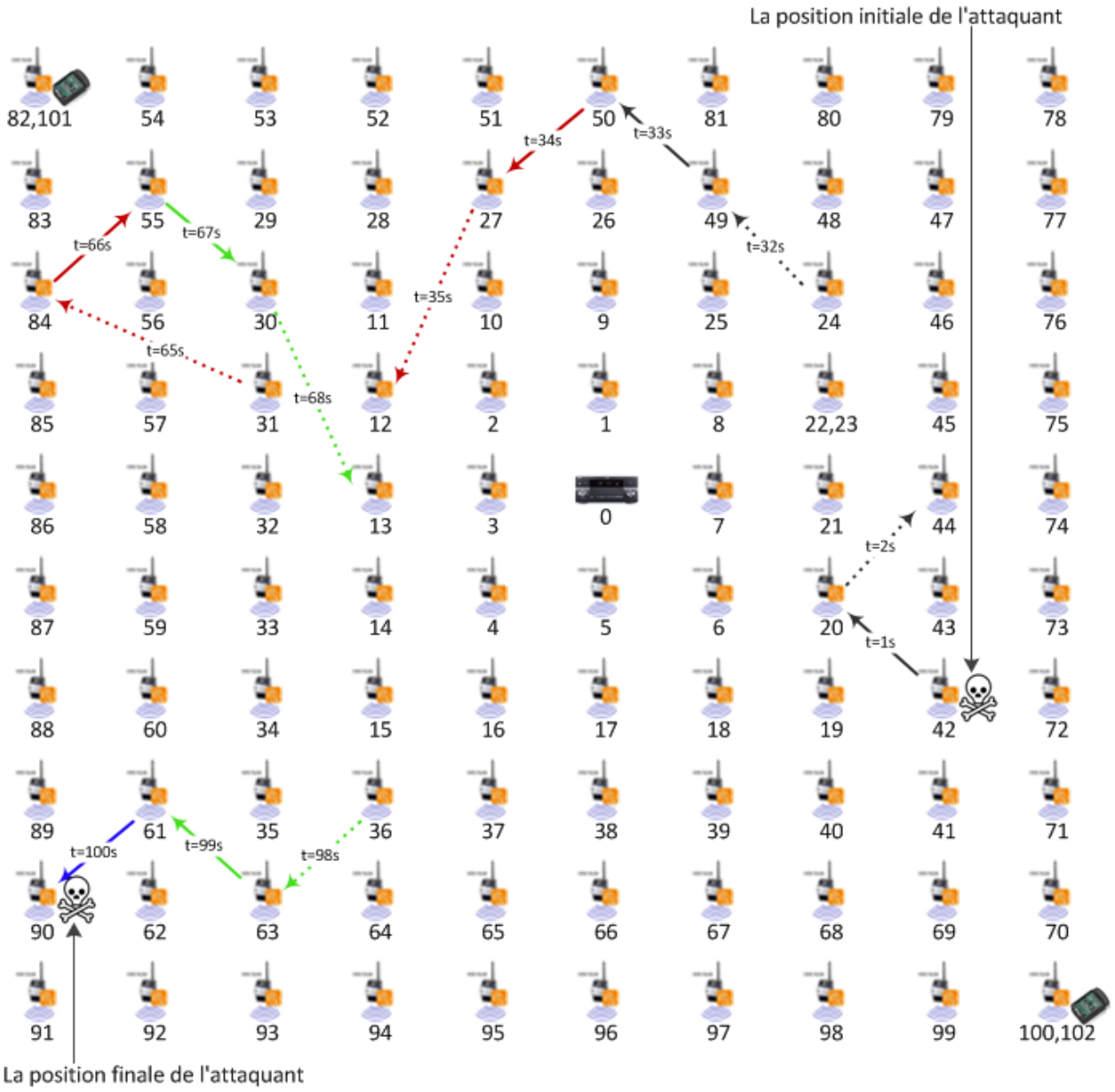

Figure 7.18 Le déplacement de l'attaquant dans le réseau des capteurs simulé WSN en fonction du temps.

Dans notre réseau simulé WSN, la position initiale de l'attaquant choisie aléatoirement (par J-Sim parmi les positions des capteurs intermédiaires) est celle du capteur numéroté 42. À l'instant $t = 1s$, l'attaquant se déplace à proximité du capteur numéroté 20, car ce capteur a le plus de trafic dans le voisinage du capteur 42 (le voisinage est composé des capteurs 19, 20, 43, 73, 72, 71, 41 et 40. Voir le tableau 5.1). De même pour les secondes suivantes, à partir de sa position courante, l'attaquant se déplace à proximité du capteur ayant le plus

de trafic dans sa région. La figure 7.18 montre le déplacement de l'attaquant dans le réseau simulé en fonction du temps.

Cette figure montre que l'attaquant se déplace vers la fausse station de base mobile. Cependant, cette fausse station de base se déplace aussi dans le réseau simulé WSN, ce qui oblige automatiquement l'attaquant à changer son parcours. Au terme de la simulation, l'attaquant se positionne à proximité de la fausse station de base et loin de la vraie station de base.

7.9 Interprétation des résultats

Suite à l'étude des figures du cas 1 (voir les figures 7.1, 7.4, 7.7, 7.10, et 7.14), du cas 2 (voir les figures 7.2, 7.5, 7.8, 7.11, et 7.15), et du cas 3 (voir les figures 7.3, 7.6, 7.9, 7.12, et 7.16), il s'avère que notre technique réussit à protéger la station de base, en créant un faux trafic plus élevé autour d'une fausse station de base mobile. De même, le trafic autour des capteurs collaborateurs est plus élevé qu'autour des autres capteurs du réseau.

Tableau 7.3 Synthèse des trois cas étudiés dans le réseau simulé et l'interprétation des résultats

Liste des figures	Similaire à la figure	Interprétation de la figure
La figure 7.2(cas 2) et 7.3 (cas3)	La figure 7.1(cas 1)	Les paquets TCP sont bien acheminés aux deux stations de base. Le faux trafic TCP étant plus élevé que le vrai trafic TCP, ce qui ne permet pas à l'attaquant de localiser la vraie station de base.
La figure 7.5(cas 2) et 7.6 (cas3)	La figure 7.4(cas 1)	Les figure démontrent que les stimuli parviennent bien à la vraie station de base.
La figure 7.8(cas 2) et 7.9 (cas3)	La figure 7.7(cas 1)	les figures démontrent que les paquets AODV parviennent bien à la fausse et à la vraie station de base.
La figure 7.11(cas 2), 7.12 (cas3), et 7.13 (cas 1 avec une trajectoire circulaire)	La figure 7.10(cas 1)	Les figures montrent le contraste entre le patron (pattern) du trafic TCP dans le réseau de capteurs sans fil WSN simulé, et les régions munies de trafic volumineux en l'occurrence la région de la fausse station de base.
La figure 7.15(cas 2), 7.16 (cas3), et 7.17 (cas 1 muni d'une trajectoire circulaire)	La figure 7.14(cas 1)	Les figures montrent le contraste entre le patron (pattern) du trafic AODV dans le réseau de capteurs sans fil WSN simulé, et les régions munies de trafic volumineux en l'occurrence la région de la fausse station de base.

Les figures 7.10 et 7.14 du cas 1, les figures 7.11 et 7.15 du cas 2, et les figures 7.12 et 7.16 du cas 3, montrent les différentes positions de la fausse station de base mobile à $t = 0s$, $t = 33s$, $t = 66s$, et $t = 99s$. La mobilité de la fausse station de base a pour résultat la création de plusieurs régions munies de trafic volumineux en messages AODV ou TCP.

Le tableau 7.3 présente une synthèse des trois cas étudiés, ainsi que les interprétations des résultats en se référant aux similitudes au cas 1. Nous constatons, par exemple, que la figure 7.2 du cas 2, et la figure 7.3 du cas 3 ont des résultats similaires à la figure 7.1 du cas 1.

7.10 Analyse des résultats de la défense d'une station de base contre les attaques d'analyse de trafic

L'analyse de trafic est une attaque ayant pour objectif la localisation d'une station de base, et son isolement du reste du réseau, ce qui rend inefficace l'ensemble du réseau et de ses capteurs. Cette attaque se base sur l'analyse de la quantité d'information en transition dans le réseau.

La génération de nouvelles régions munies de trafic plus élevé que celui de la région de la vraie station de base, est l'une des techniques [40] de protection contre cette attaque d'analyse de trafic. Lors de notre étude, nous avons créé de nouvelles régions avec un trafic élevé autour d'une fausse station de base mobile recevant du faux trafic. Pour cela, un réseau de 100 capteurs est déployé sur une région de 1500×1500 unité. Parmi ces 100 capteurs, il y a s capteurs générant du faux trafic destiné à la fausse station de base. Cette dernière est choisie aléatoirement parmi les capteurs du réseau, qui sont au moins à h sauts de la vraie station de base.

Les résultats de la simulation du réseau de notre étude permettent de confirmer que les nouvelles régions de la fausse station de base ont un trafic plus important que celui de la vraie station de base. Notre technique permet alors de disperser l'attention de l'attaquant, et ainsi de protéger la vraie station de base de l'attaque d'analyse de trafic, tel que illustré par la figure 7.18 .

Notre technique est utilisée dans le cas d'un réseau muni d'une seule station de base, mais elle peut être généralisée à des réseaux ayant plusieurs stations de base, en créant autant de fausses stations de base que de vraies stations de base.

L'utilisation d'une fausse station de base mobile permet de générer plusieurs régions volumineuses en trafic. À chaque saut, l'attaquant essaye de localiser la région ayant le volume de trafic le plus élevé, en supposant que cette région demeure la même dans tous les cas exposés. Cependant, à chaque saut, la fausse station de base se déplace et modifie ainsi la quantité de volume de trafic échangé partout dans le réseau, ce qui perturbe l'évolution de l'attaquant, qui doit recalculer sa démarche. Cette solution est plus efficace que celle de la défense utilisant une fausse station de base statique, car elle retarde l'attaquant dans sa recherche de la vraie station de base.

Il existe plusieurs techniques de randomisation de la position de la fausse station de base mobile. Cette fausse station de base peut se déplacer, par exemple, dans une trajectoire circulaire d'un rayon de h sauts autour de la vraie station de base. Avec ce type de déplacement, la fausse station de base se construit des régions avec trafic élevé autour de la vraie station de base. Ainsi, l'attaquant d'analyse de trafic peut se rapprocher de la vraie station de base, mais il reste toujours à plus de h sauts de celle-ci.

7.11 Le coût de l'énergie de la défense

La figure 7.19 a pour coordonnées (en x-abscisse) le temps de simulation, et (en y-ordonnée) la quantité de l'énergie totale résiduelle des capteurs du réseau simulé en pourcentage de l'énergie initiale totale du réseau. L'énergie résiduelle est calculée avec une périodicité de 5 secondes.

La figure 7.19 montre les cas suivants :

- Un réseau WSN, sans défense ne subissant pas d'attaque d'analyse de trafic, à $t = 100s$, possède une énergie résiduelle totale de 80% de l'énergie totale initiale.
- Un réseau WSN, sans défense subissant une attaque d'analyse de trafic, s'arrête de fonctionner totalement à $t = 50s$ à cause de la découverte de la station de base. Dans ce cas, l'énergie résiduelle totale est sans importance.
- Un réseau WSN, avec défense ($h = 4$, $s = 8$) et subissant une attaque d'analyse de trafic, à $t = 100s$, possède une énergie résiduelle totale de 40% de l'énergie totale initiale.
- Un réseau WSN, avec défense ($h = 3$, $s = 8$) et subissant une attaque d'analyse de trafic, à $t = 100s$, possède une énergie résiduelle totale de 20% de l'énergie totale initiale.
- Un réseau WSN, avec défense ($h = 3$, $s = 12$) et subissant une attaque d'analyse de trafic, dès $t = 85s$, a une énergie résiduelle totale de 0% de l'énergie totale initiale.

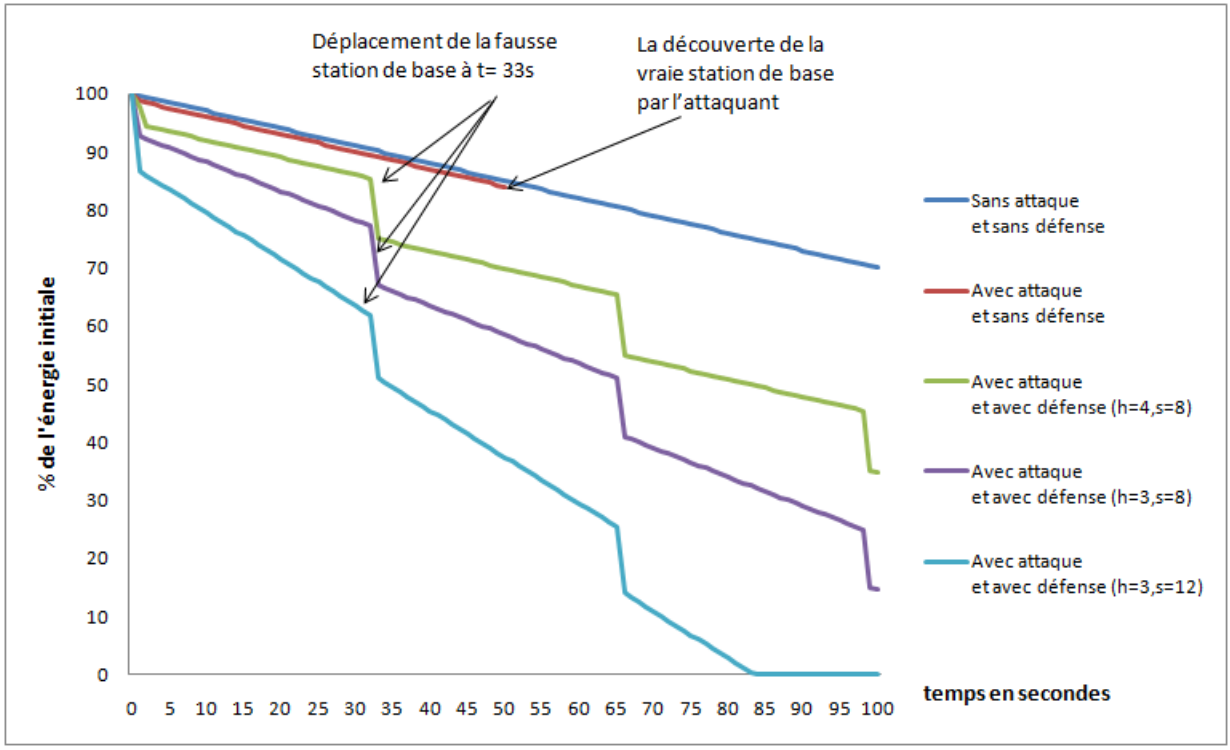

Figure 7.19 La consommation de l'énergie totale des capteurs du réseau WSN selon le scénario de la défense

Nous remarquons que l'énergie est mieux consommée dans le cas où il n'y a ni défense ni attaque, cependant ce cas est idéal et irréaliste. Il est clair aussi qu'un réseau protégé dure plus longtemps qu'un réseau sans défense. Nous constatons aussi que la durée de vie du réseau protégé est plus grande avec h plus grand, de même cette durée de vie est plus grande avec s plus petit. En effet, quand la valeur de s est petite, peu de capteurs intermédiaires sont sources de faux trafic, et nécessitent donc une moindre consommation en énergie.

Il est donc intéressant de choisir une valeur pour le paramètre h qui ne soit pas petite, et une petite valeur pour le paramètre s qui doit être assez grande pour générer un faux trafic plus élevé que le vrai trafic dans le réseau WSN.

Concernant la technique de mobilité de la fausse station de base, dans une trajectoire circulaire autour de la vraie station de base avec un rayon de h sauts, la valeur de h ne doit être ni grande ni très petite, et la valeur de s ne doit être ni minime ni grande. Ainsi, la consommation de l'énergie reste modérée.

7.12 Test de la défense dans un réseau WSN de m vraies stations de base ($m > 1$)

La technique de génération et d'utilisation de faux trafic, reçus par une fausse station de base, peut être utilisée aussi dans un réseau de capteurs WSN muni de plusieurs vraies stations de base. Cependant cette technique doit être réadaptée en choisissant m différentes fausses stations de base où chaque fausse station de base correspond à une vraie station de base, et reçoit du faux trafic de s capteurs positionnés à h sauts.

Nous avons re-simulé le même réseau de capteurs WSN étudié auparavant, mais en y ajoutant deux nouvelles stations de base. Nous avons reconsidéré les 3 cas précédents, mais en élisant, pour chacun des cas, deux nouvelles fausses stations de base, et s capteurs à h sauts des vraies stations de base correspondantes.

Les résultats de la simulation du réseau de m stations de base ressemblent à ceux d'un réseau muni d'une seule station de base. Ils confirment que la technique d'utilisation de m fausses stations de base mobiles est efficace contre l'attaque d'analyse de trafic dans un réseau WSN de m vraies stations de base.

En effet, l'attaquant d'analyse de trafic, reconnaissant l'existence de m vraies stations de base, cherche à s'approcher d'une des m régions de trafic élevé, mais il ne peut remarquer que celles des m régions des fausses stations de base avec l'illusion, qu'il s'agit des m vraies stations de base.

7.13 Conclusion

Au cours de ce chapitre, nous avons simulé notre nouvelle technique de défense contre l'attaque d'analyse de trafic, qui utilise du faux trafic TCP reçu par une fausse station de base mobile. La simulation avec J-Sim nous permet de confirmer que notre technique est valide pour un réseau WSN muni d'une seule vraie station de base, et aussi pour un réseau WSN ayant m vraies stations de base.

Suite à nos simulations, nous concluons qu'afin d'optimiser l'utilisation de l'énergie, il est nécessaire d'utiliser une grande valeur pour le paramètre h, et une petite valeur pour le paramètre s.

CHAPITRE 8

CONCLUSION

Nous avons présenté une nouvelle technique permettant de défendre une station de base contre l'attaque d'analyse de trafic, en utilisant du faux trafic et une fausse station de base mobile.

8.1 Synthèse des travaux

Notre étude élabore une nouvelle approche de protection contre les attaques de dénis de service, et plus particulièrement l'attaque d'analyse de trafic AAT, faisant appel à des méthodes de quantifications des paquets en transition dans le réseau WSN.

- Nous avons introduit l'utilisation de certains capteurs générant du faux trafic TCP.
- Nous avons élu aléatoirement $m = 1$ fausse station de base. Chacune des m fausses stations de base doit être au moins à h sauts de la vraie station de base correspondante (h est un paramètre de la simulation du réseau WSN).
- Nous avons déplacé dynamiquement, et aléatoirement une fausse station de base.
- Nous avons généré un faux trafic à destination d'une fausse station de base. Ce faux trafic doit être aussi important que le vrai trafic à destination de la vraie station de base.
- Nous avons généré ce faux trafic aléatoirement dans plusieurs régions du réseau, afin de perturber la recherche de l'attaquant, qui conclut que la région munie d'un trafic volumineux serait la région de la vraie station de base.
- Nous avons appliqué notre technique sur un réseau muni d'une seule station de base, ainsi que sur un autre réseau de capteurs WSN muni de plusieurs stations de base.

Les différents tests décrits dans le chapitre 7, créditent cette nouvelle technique de diversion, qui permet la protection de la station de base contre les attaques d'analyse de trafic.

8.2 Contributions des travaux

Les travaux existants ont démontré le rôle de l'introduction de faux trafic [5], dans la défense contre l'attaque d'analyse de trafic. L'innovation de notre étude consiste à utiliser une fausse station de base ***mobile*** recevant du faux trafic, au lieu d'envoyer ce faux trafic à partir d'un capteur vers ses voisins. Notre contribution consiste à créer une fausse station

de base recevant du faux trafic, et de la mobiliser pour perturber la démarche de l'attaquant dans sa recherche de la vraie station de base.

La fausse station de base peut être mobile sur une trajectoire aléatoire, ou sur une trajectoire circulaire de rayon h sauts.

8.3 Limitations de la solution proposée

Notre nouvelle technique est très utile pour la protection de la station de base contre l'attaque d'analyse de trafic, mais elle demeure limitée par la consommation additionnelle en énergie, de la fausse station de base et des capteurs générant du faux trafic.

En effet, la génération de faux trafic par des capteurs, requiert une consommation additionnelle en énergie non négligeable. De même, chaque déplacement de la fausse station de base consomme de l'énergie. Cette énergie, nécessaire pour le déplacement de la fausse station de base, et pour l'envoi de faux trafic par les capteurs collaborateurs, fait diminuer l'énergie totale disponible pour le réseau, et par conséquent, cette consommation additionnelle d'énergie réduit la durée de vie initiale du réseau de capteurs WSN.

Cette durée de vie est maximale dans le cas d'un réseau de capteurs ne subissant pas d'attaque d'analyse de trafic. Cependant, cette durée de vie se réduit par la mise en panne du réseau par un attaquant d'analyse de trafic. Il est utile de noter que la durée de vie d'un réseau protégé est plus longue que celle d'un réseau attaqué.

8.4 Améliorations futures

La prochaine étape consisterait à étudier l'impact de notre technique sur la consommation totale de l'énergie de l'ensemble des capteurs d'un réseau WSN, et de conclure à un déplacement de la fausse station de base, et à une génération de faux trafic moins onéreux en énergie. Il serait utile de vérifier si le faux trafic devrait être généré par certains capteurs qui ne sont pas très sollicités par l'acheminement du vrai trafic, comme les capteurs situés loin de la vraie station de base et par lesquels ne passent que de petites quantités d'informations.

Notre défense de faux trafic, utilisant une fausse station de base mobile, pourrait être activée seulement lorsqu'un attaquant de l'analyse de trafic est détecté, ce qui permettrait d'économiser de l'énergie. La problématique est de trouver une manière d'identifier cet attaquant.

RÉFÉRENCES

[1] D.R. Raymond and S.F. Midkiff. Denial-of-service in wireless sensor networks : Attacks and defenses. Pervasive Computing, IEEE, 7(1) :74 –81, jan.-march 2008.

[2] "Google". "google.ca,". "http ://images.google.ca/", "consulte le 5 sep 09".

[3] Wood A. D. and Stankovic J. A. A taxonomy for denial-ofservice attacks in wireless sensor networks. Handbook of Sensor Networks : Compact Wireless and Wired Sensing-Systems, 2005.

[4] A.S.K. Pathan, Hyung-Woo Lee, and Choong Seon Hong. Security in wireless sensor networks : issues and challenges. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, volume 2, pages 6 pp. –1048, feb. 2006.

[5] Jing Deng, Richard Han, and Shivakant Mishra. Countermeasures against traffic analysis attacks in wireless sensor networks. Security and Privacy for Emerging Areas in Communications Networks, International Conference on, 0 :113–126, 2005.

[6] A. Sobeih, J.C. Hou, Lu-Chuan Kung, Ning Li, Honghai Zhang, Wei-Peng Chen, Hung-Ying Tyan, and Hyuk Lim. J-sim : a simulation and emulation environment for wireless sensor networks. Wireless Communications, IEEE, 13(4) :104 –119, aug. 2006.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks : a survey. Computer Networks, 38(4) :393 – 422, 2002.

[8] Kemal Akkaya and Mohamed Younis. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, 3(3) :325 – 349, 2005.

[9] O. Younis, M. Krunz, and S. Ramasubramanian. Node clustering in wireless sensor networks : recent developments and deployment challenges. Network, IEEE, 20(3) :20 – 25, may-june 2006.

[10] Chonggang Wang, K. Sohraby, Yueming Hu, Bo Li, and Weiwen Tang. Issues of transport control protocols for wireless sensor networks. In Communications, Circuits and Systems, 2005. Proceedings. 2005 International Conference on, volume 1, pages 422 – 426 Vol. 1, May 2005.

[11] W. N. Gangsterer M. J. Khan and G. Haring. Congestion avoidance and energy efficient routing protocol for wireless sensor networks with a mobile sink. Journal of Networks, 2(6) :42, 2007.

[12] J. Zhao, R. Govindan, and D. Estrin. Computing aggregates for monitoring wireless sensor networks. In Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on, pages 139 – 148, May 2003.

[13] Yogesh Sankarasubramaniam, Özgür B. Akan, and Ian F. Akyildiz. Esrt : event-to-sink reliable transport in wireless sensor networks. In Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, MobiHoc '03, pages 177–188, New York, NY, USA, 2003. ACM.

[14] L. Li and J.Y. Halpern. Minimum-energy mobile wireless networks revisited. In Communications, 2001. ICC 2001. IEEE International Conference on, volume 1, pages 278 –283 vol.1, June 2001.

[15] Fan Xiangning and Song Yulin. Improvement on leach protocol of wireless sensor network. Sensor Technologies and Applications, International Conference on, 0 :260–264, 2007.

[16] K. Sohrabi, J. Gao, V. Ailawadhi, and G.J. Pottie. Protocols for self-organization of a wireless sensor network. Personal Communications, IEEE, 7(5) :16 –27, October 2000.

[17] Ruizhong Lin, Zhi Wang, and Youxian Sun. Energy efficient medium access control protocols for wireless sensor networks and its state-of-art. In Industrial Electronics, 2004 IEEE International Symposium on, volume 1, pages 669 – 674 vol. 1, May 2004.

[18] Sung-Chul Jung and Hyoung-Kee Choi. An energy-aware routing protocol considering link-layer security in wireless sensor networks. In Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on, volume 01, pages 358 –361, feb 2009.

[19] David Curren. A survey of simulation in sensor networks. Architecture, pages 867–872, 2008.

[20] Virgil D. Gligor. A note on the denial-of-service problem. Proceedings of IEEE Symposium on Security and Privacy, pages 139 –149, 1983.

[21] Virgil D Gligor. A note on the denial-of-service problem. Proceedings of IEEE Symposium on Security and Privacy, pages 139–149, 1983.

[22] A.D. Wood and J.A. Stankovic. Denial of service in sensor networks. Computer, 35(10) :54 – 62, October 2002.

[23] R. D. Gitlin E. Ayanoglu, Chih-Lin I and J. E. Mazo. Diversity coding for transparent self-healing and fault-tolerant communication networks. IEEE Trans. Commun, pages 1677–1686, 1993.

[24] Nael Abu-Ghazaleh, Kyoung-Don Kang, and Ke Liu. Towards resilient geographic routing in wsns. In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Q2SWinet '05, pages 71–78, New York, NY, USA, 2005. ACM.

[25] Chris Karlof and David Wagner. Secure routing in wireless sensor networks : attacks and countermeasures. Ad Hoc Networks, 1(2-3) :293 – 315, 2003. Sensor Network Protocols and Applications.

[26] Y.-C. Hu, A. Perrig, and D.B. Johnson. Packet leashes : a defense against wormhole attacks in wireless networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, volume 3, pages 1976 – 1986 vol.3, april 2003.

[27] Newso James, Elaine Shi, Dawn Song, and Adrian Perrig. The sybil attack in sensor networks : analysis & defenses. In Proceedings of the 3rd international symposium on Information processing in sensor networks, IPSN '04, pages 259–268, New York, NY, USA, 2004. ACM.

[28] John Douceur. The sybil attack. In Peter Druschel, Frans Kaashoek, and Antony Rowstron, editors, Peer-to-Peer Systems, volume 2429 of Lecture Notes in Computer Science, pages 251–260. Springer Berlin / Heidelberg, 2002.

[29] Newso James, Elaine Shi, Dawn Song, and Adrian Perrig. The sybil attack in sensor networks : analysis & defenses. In Proceedings of the 3rd international symposium on Information processing in sensor networks, IPSN '04, pages 259–268, New York, NY, USA, 2004. ACM.

[30] A. Price, K. Kosaka, and S. Chatterjee. A key pre-distribution scheme for wireless sensor networks. In Wireless Telecommunications Symposium, 2005, pages 253 – 260, 2005.

[31] Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In Proceedings of the 2nd ACM workshop on Wireless security, WiSe '03, pages 1–10, New York, NY, USA, 2003. ACM.

[32] P. Nikander T. Aura and J. Leiwo. Dos-resistant authentication with client puzzles. Proc. Security Protocols Workshop 2000, Springer-Verlag, New York, 13(4) :170–177, august 2000.

[33] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, MobiHoc '05, pages 46–57, New York, NY, USA, 2005. ACM.

[34] Julius Degesys, Ian Rose, Ankit Patel, and Radhika Nagpal. Desync : self-organizing desynchronization and tdma on wireless sensor networks. In Proceedings of the 6th international conference on Information processing in sensor networks, IPSN '07, pages 11–20, New York, NY, USA, 2007. ACM.

[35] Scott A. Crosby and Dan S. Wallach. Denial of service via algorithmic complexity attacks. In Proceedings of the 12th conference on USENIX Security Symposium - Volume 12, pages 3–3, Berkeley, CA, USA, 2003. USENIX Association.

[36] Xi Luo, Xu Ji, and Myong-Soon Park. Location privacy against traffic analysis attacks in wireless sensor networks. In Information Science and Applications (ICISA), 2010 International Conference on, pages 1 –6, april 2010.

[37] Ying Jian, Shigang Chen, Zhan Zhang, and Liang Zhang. A novel scheme for protecting receiver's location privacy in wireless sensor networks. Wireless Communications, IEEE Transactions on, 7(10) :3769 –3779, october 2008.

[38] Jing Deng, Richard Han, and Shivakant Mishra. Countermeasures against traffic analysis attacks in wireless sensor networks. Security and Privacy for Emerging Areas in Communications Networks, International Conference on, 0 :113–126, 2005.

[39] Xi Luo, Xu Ji, and Myong-Soon Park. Location privacy against traffic analysis attacks in wireless sensor networks. In Information Science and Applications (ICISA), 2010 International Conference on, pages 1 –6, april 2010.

[40] Jing Deng, Richard Han, and Shivakant Mishra. Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks. Dependable Systems and Networks, International Conference on, 0 :637, 2004.